Blind Sided

A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone

Blind Sided

A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone

Authors:
Ashley Mattheis
Daveed Gartenstein-Ross
Varsha Koduvayur
Cody Wilson

February 2023

IRREGULAR WARFARE CENTER

www.IrregularWarfareCenter.org

Arlington, VA

About the Authors

Dr. Ashley Mattheis is a scholar, lecturer, and research consultant. Her work brings together cultural studies, media studies, and rhetorical criticism to explore topics such as the visual rhetoric of far-right extremist propaganda and the impact of digital technology and media on democratic culture. Her publications include "Does the Institution have a Plan for That?: Researcher Safety and the Ethics of Institutional Responsibility," in *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, and *'The Greatness of Her Position': Comparing Identitarian and Jihadi Discourses on Women*, a report published by the International Centre for the Study of Radicalisation. Dr. Mattheis recently worked as a visiting researcher at the Cyberthreats Research Centre (CYTREC) at Swansea University, studying extremist use of Telegram. She also produces public-facing scholarship through fellowships with the U.K.-based Centre for Analysis of the Radical Right and the U.S.-based Institute for Research on Male Supremacism. She has previously been an Associate Fellow with the Global Network on Extremism and Technology (GNET). Dr. Mattheis holds a Ph.D. in communication from the University of North Carolina at Chapel Hill.

Dr. Daveed Gartenstein-Rossis a scholar, author, practitioner, and entrepreneur who is the founder and chief executive officer of Valens Global. Dr. Gartenstein-Ross has been described by the director of the U.S. Department of Defense's Strategic Multilayer Assessment program as "the expert that the experts call to discuss the nettlesome challenges with terrorism and counterterrorism." In addition to leading Valens Global, Dr. Gartenstein-Ross serves as a senior advisor on asymmetric warfare at the Foundation for Defense of Democracies and an associate fellow at the International Centre for Counter-Terrorism – The Hague, and is a faculty member at both Carnegie Mellon University and Duke University. He has previously held positions with the U.S. Department of Homeland Security, Google's tech incubator Jigsaw, and Georgetown University. Dr. Gartenstein-Ross has led several major projects focusing on strategic communications and disinformation, including working as a European Union-appointed strategic communications expert to train Nigerian civil-society activists on militant groups' use of the online space; mapping the online counter-ISIS narrative space for Google's Redirect Method; and assessing the impact of counter-messaging campaigns for the U.S. State Department's Global Engagement Center. Dr. Gartenstein-Ross has testified before the European Parliament, Canadian House of Commons, U.S. Senate, and U.S. House of Representatives on relevant topics. He holds a Ph.D. in world politics from the Catholic University of America and a J.D. from the New York University School of Law.

About the Authors

Ms. Varsha Koduvayur is a senior analyst in the Strategic Futures and Research program at the Irregular Warfare Center. In this role, she conducts research on irregular warfare and its evolution, and supports the Center's publication efforts. She is also a research manager at Valens Global. Prior to joining Valens, Ms. Koduvayur was a senior research analyst at the Foundation for Defense of Democracies, where she covered the Gulf Arab states. Her work has appeared in *Foreign Policy*, *Foreign Affairs*, and *CNN Business*, among other outlets. Ms. Koduvayur holds a B.A. in international relations and Arabic from Michigan State University.

Mr. Cody Wilson contributed to this report while working as an analyst at Valens Global. He holds a master's degree in global studies and international relations, with a concentration in conflict resolution, from Northeastern University. Mr. Wilson previously earned a bachelor's degree in political science with a concentration in international relations from the University of California, Los Angeles. During his time at Valens, Mr. Wilson contributed to reports used in federal litigation, helped execute eight successful wargames, designed a cybersecurity-focused tabletop exercise, and produced reports for the U.S. government.

Table of Contents

Table of Contents

Glossary

affordances: In the new media sphere context, *affordances* are sets of features specific to particular software or platforms. Users often utilize these features in ways that developers did not plan.

bots: Short for *robots*, bots are automated programs that perform repetitive tasks and can be designed to mimic the online activity of humans.

disinformation: Media that contains false or misleading information that is created and shared to intentionally harm a specific target.

gamification: The process of adding "game" elements, such as leaderboards and rewards systems, to non-game environments.

gray zone competition: The *gray zone* is the space between war and peace. Gray zone competition can be thought of as competition between actors (state or non-state) that exceeds normal peacetime competition but does not meet the threshold of a declared war.

hashtag hijacking: Using an existing popular hashtag to circulate unrelated content.

information environment: The full spectrum of actors and systems that share and use information.

information operations (IOs): Information operations use information to target an audience with a specific message to create a desired change within that audience.

malinformation: Information that is based on truth but is exaggerated or otherwise taken out of context to cause harm.

meme: A term describing how small bits of cultural information are passed between people, replicated over and over, and spread widely.

memeification: The process of turning a piece of content (e.g., taglines, images, song snippets, cultural icons) into a meme.

misinformation: Media that contains false or misleading information but that is not intentionally shared to cause harm. Often the sharer is unaware that the media contains false or misleading information.

new media ecosystem: Traditional, digital, and social media in an interrelated ecosystem that allows participants to be sources, producers, and consumers of information, often simultaneously.

polluted information: A catch-all term for disinformation, misinformation, and malinformation.

sockpuppet accounts: Fake social media accounts that are meant to appear real to other users.

Introduction

In June 2022, Facebook and Twitter accounts suddenly focused their wrath on Australian company Lynas. The previous year, Lynas—the largest rare earths mining and processing company outside China—had inked a deal with the U.S. Department of Defense to build a processing facility for rare earth elements in Texas. Over a year after the deal was signed, concerned Texas residents began taking to social media to loudly voice opposition to the deal. They claimed the facility would create pollution and toxic waste, endangering the local population. Residents disparaged Lynas's environmental record, and called for protests against the construction of the processing facility and a boycott of the company.

Only these posts weren't coming from Texas residents at all. The lead voices on the topic weren't even real identities. The campaign was led by fake accounts set up and maintained by the People's Republic of China (PRC) in an information operation (IO) aimed at smearing the image of China's competitors in the field of rare earths—metals critical to producing advanced electronics, electric vehicles, batteries, and renewable energy systems. China is a behemoth in this field, controlling over 80% of global production of rare earths, and is eager to maintain its supply chain dominance.[1]

This PRC-led campaign against a rival in the rare earths field was discovered by cybersecurity firm Mandiant, which has also unearthed past PRC-led IOs aimed at promoting "narratives in support of the political interests of" Beijing.[2] Nor was Lynas the only company that China targeted in its attempts to use the information space to ensure continued rare earths dominance. In June 2022, the same PRC-led campaign targeted both Appia Rare Earths & Uranium Corporation, a Canadian rare earths mining company, and the American rare earths manufacturer USA Rare Earth. Both companies were bombarded by "negative messaging in response to potential or planned rare earths production activities," Mandiant noted.[3]

Examples of posts created by the Chinese influence operation against Lynas. Source: Mandiant.

China's desired end was to damage Western companies in the rare earths sector to thwart would-be competitors. In doing so, Beijing seeded a social media operation, using accounts carefully crafted to look like Texas residents voicing very real fears about the damage Lynas could do to their communities.

China's information operations—and, indeed, information operations in general—are not a new phenomenon. But IOs have metamorphosed and become turbocharged in today's digital information environment. As Thomas Rid has observed, such operations have been "reborn and reshaped by new technologies and internet culture."[4]

Characteristics of the digital-age information environment allow various actors to leverage information operations to propagate information and mobilize audiences for their own ends (or alternatively, to *suppress* the spread of information or mobilization of populations, as we will discuss).

This dynamic has a deep influence on how information operations are conducted in the gray zone, which is the space that exists between war and peace. *Gray zone competition* can be thought of as competition between actors (state or non-state) that exceeds normal peacetime competition but does not meet the threshold of a declared war. The "gray zone" is synonymous with irregular warfare. Modern information operations are favored by gray zone actors because they allow competition with adversaries without direct physical confrontation. To carry out gray zone information operations, actors rely on and exploit psychological biases, social and political structures, characteristics and affordances of the media and information environments, and emerging technologies. Further enabling gray zone information operations is the *new media ecosystem*, which comprises traditional, digital, and social media in an interrelated ecosystem that allows participants to be sources, producers, and consumers of information, often simultaneously.

This report uses the framing of *ends, ways,* and *means* to analyze the impact of information operations.[5] By *ends*, we refer to the end state or outcome that information operations actors are seeking to achieve—in other words, why the actor is conducting the IO in the first place. Ultimately, all information operations have a desired end, be it political, economic, diplomatic, or social. By *ways*, we refer to how actors seek to achieve their preferred end through information operations (including by amplifying or suppressing information). And by *means*, we refer to the specific information operation that the IO actor employs—in other words, the specific "play" that they select from the IO playbook that this report presents. IO actors have a number of tools at their disposal to conduct the IO, which provide the methods, capabilities, and resources for conducting information operations.

Policymakers and security professionals in liberal democracies have repeatedly been blindsided by emerging gray zone IO threats, while their focus has been on *past* IOs they have encountered. This report's ambitious goal is to take a significant step toward changing this dynamic by de-centering the prevailing analytic focus on the *actors* employing information operations. Instead, the report focuses on the *strategies* and *tools* that actors employ in their information operations to achieve their desired end state. When analysts are overly focused on the activities of a particular actor, they open themselves up to being blindsided. After all, in this information environment, no actor formulates its IOs in a vacuum. For example, when a left-wing movement successfully mobilizes large numbers of people to the streets in protest, its success is studied not only by that movement's adherents, but also by white supremacists, pro-democracy social movements in the Middle East, authoritarian states seeking to exacerbate social divisions in the West, jihadist groups, and other actors. *Successful IOs and strategies are replicated not only by the actor that pioneered them and by its allies, but also by a multiplicity of other actors with various ideologies, motivations, and goals*.

The report makes three primary contributions. **First**, it offers the *propagation-mobilization framework* for understanding IOs in the gray zone. This framework holds that there are two ways IOs are used in gray zone strategies—propagation of information and mobilization to action—to achieve a desired end. Gray zone IOs can be understood as having one of two impacts on these lines of effort, creating either positive or negative feedbacks that amplify or suppress propagation and mobilization to action. Though this framework may appear at first blush to be a simplifying schema, we believe it in fact has revolutionary implications, as this report details later. **Second**, this report adapts evolutionary theory to enhance our analytic understanding of information operations in the gray zone. Evolutionary theory has previously been employed in certain contexts in the social sciences, but we assess it as uniquely valuable for illuminating information operations.

Third, this report outlines a robust range of digital and offline IOs, explicates their utility for a variety of actors, and maps their interactive potential. It provides a "playbook" for understanding information operations as a critical means to gray zone competition. In doing so, we seek to create understanding of how gray zone actors employ information operations. The impact of such an elucidation may at first seem simple, but we believe that it will have a potentially profound effect. In pulling together various and seemingly disparate IOs into one binding framework, we hope to provide a richer understanding of IOs than that conveyed by actor-focused analyses, which will potentially overlook the evolutionary nature of IOs and thus possibly miss emergent IO threats.

Our endeavor here is similar to that undertaken by the iconic chess theorist Aron Nimzowitsch, whose 1925 volume *My System* worked to discern principles and hence a framework for understanding the complex war being fought on the 64 squares of the chessboard. As Nimzowitsch detailed:

> The individual items, especially in the first part of the book, are seemingly very simple—but that is precisely what is meritorious about them. Having reduced the chaos to a certain number of rules involving inter-connected causal relations, that is just what I think I may be proud of. How simple the five special cases in the play on the seventh and eighth ranks sound, but how difficult they were to educe from the chaos! Or the open files and even the pawn chain! .... I now hand this first installment over for publication. I do so in good conscience. My book will have its defects—I was unable to illuminate all the corners of chess strategy—but I flatter myself of having written the first real textbook of chess and not merely of the openings.[6]

We believe we are, in a similar fashion, creating a playbook for understanding information operations in the gray zone. Our aim is to provide a clear framework in which IOs can be understood and—more importantly—predicted, by concretely discerning the IO strategies and tactics that actors may deploy, and noting their interlinkages and evolutions. While no such summary can be exhaustive of all potential IOs, particularly given the ever-changing technological context and the creative capacity of gray zone actors, the depth of this summary offers an essential overview of the utilities, modalities, and capacities embedded in contemporary gray zone IO competition.

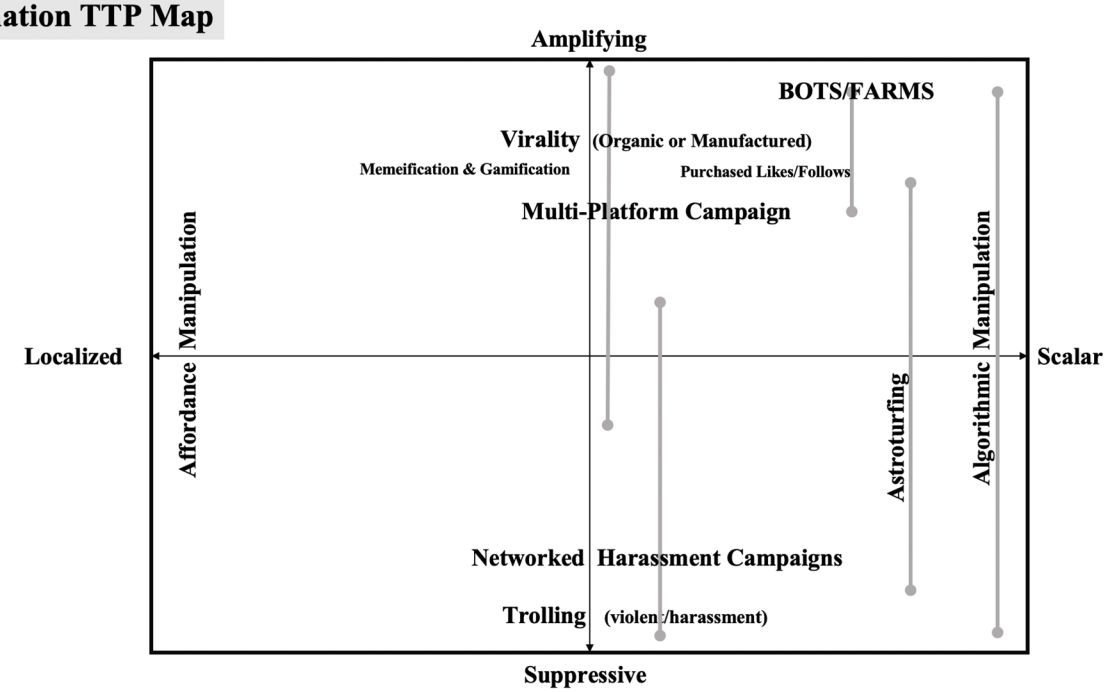
To provide a roadmap of this report, after describing the modern information environment and its role in enabling gray zone IOs, we lay out our framework in full. Drawing on the work of Canadian scholar Yannick Veilleux-Lepage, who recently published a book applying evolutionary theory to airplane hijackings, we similarly apply evolutionary theory to information operations.[7] This report also divides IOs into the two distinct lines of effort (LOEs) of propagation and mobilization. Propagation and mobilization LOEs can operate independently or feed into one another, producing feedback loops. The outcome of both propagation and mobilization can be either amplifying or suppressive. The desired outcome shapes which IOs will be selected for a particular LOE.

Amplifying propagation is rather intuitive: doing so is intended to rapidly spread information through the new media ecosystem. By contrast, *suppressive propagation* is the silencing of information in the new media ecosystem, which can come from account takedowns, censorship (including producing an environment of self-censorship), harassment, or other means of preventing information from spreading. Similarly, *amplifying mobilization* is one of the classic goals of IOs, to make a target population go out and do something, such as donating blood, voting, protesting, carrying out terrorist attacks, or storming the U.S. Capitol. *Suppressive mobilization* aims to prevent people from doing something, such as staying home instead of voting, refraining from going to ISIS's caliphate, declining to join a gang, or declining to take a COVID-19 vaccine.[8]

Using this report's framework, we discuss the varieties of propagation and mobilization IOs, how these IOs are adapted across technology platforms and by users, and how these IOs are transmitted to other actors. This allows for a better understanding of how some IOs predominate while others die off. Our framework also allows for

analysis of "selection factors," which can be broken down into the categories of *feasibility, legitimacy*, and *effectiveness*. Feasibility is a selection factor that considers how readily a particular IO can be carried out within a particular context; legitimacy gauges how well the information or mobilization strategies resonate with the target audience; and effectiveness measures whether the propagation or mobilization lines of effort have the intended effect.

Information TTP Map



The propagation-mobilization framework also has other implications. While mobilization is generally well defined in the literature, propagation's role is an important departure from analysis of IOs that focuses on "fake news," including disinformation. In place of such concepts, this report uses *propagation of perspective* as a value-neutral term to describe information intended to shape an audience's perspective. The propagation of perspective is a socio-technical process that utilizes information and cultural relations to achieve strategic goals. We may see these goals as noble or malign; but we should understand that a variety of actors with differing and often directly conflicting goals are watching and learning from one another. They are, often unintentionally, sharing IOs. Unlike the concepts of fake news or disinformation, propagation of perspective recognizes the complexity of the new media ecosystem and the myriad ways that information travels in that ecosystem. The socio-technical processes that enable propagation of perspective draw upon interactivity, convergence, and access to vast quantities of data to circulate information through the media ecosystem.

To highlight how this works, we examine the debate surrounding the origins of COVID-19 to showcase how information is propagated through the new media ecosystem, including how certain theories about COVID-19's origins were amplified while others were suppressed. The complex and multifaceted nature of how perspective propagates is on full display as we describe the ways in which legitimate information and perspective were ensnared in purges of conspiracy theories.

By applying the propagation-mobilization framework to gray zone IOs, we examine new media IOs that manipulate communication technologies like digital and social media to propagate information rapidly to a potentially enormous audience. Such manipulation can be achieved in localized operations or at scale. Localized IOs include affordance manipulation and evasive tactics. Scalar IOs include multi-platform operations and algorithmic manipulation.

The propagation-mobilization framework also allows us to examine how IOs can mobilize a target audience. Mobilization repertoires include online actions related to the interactivity of digital and social media, including circulation-based IOs such as interactive circulation, intermediation, and reactive circulation, as well as suppressive IOs like doxxing, networked swarms, brigading, and swatting. Mobilization repertoires also include offline actions such as non-violent protests, movements, and events, and also violent versions of each. Importantly, these action IOs, both online and offline, have been developed in large part by everyday people rather than by professionals trained to deploy information operations.

These mobilization IOs become exploitable by gray zone actors precisely because they are responses and actions that people already consider appropriate in the context of socio-political engagement. Gray zone IOs may thus lead to what appears to be grassroots mobilization that has in fact been manipulated by outside actors, a practice known as *astroturfing*. The campaign against Lynas introduced at the beginning of this report is an example of astroturfing. Moreover, threat actors may try to coopt existing movements or manipulate their mobilization.

Gray zone IOs are likely to increase in frequency, scope, and sophistication. With further technological innovation, IOs will likely become tougher to detect. Moreover, technological and social developments have rendered a state's population more vulnerable to targeting by IO actors than in years past. As we will show in this report, the new media ecosystem has also drastically shrunk the time between propagation of information and mobilization to action—a shrinkage that IO actors will seek to exploit. The time for states and societies to build resilience to gray zone IOs is now.

Hostile actors' IOs represent a serious threat to democracy. Such IOs seek to fray the fabric of trust and tolerance that binds states, societies, communities, and institutions together. Hostile actors are able to do so for a relatively low cost. Thus, we view this report's admittedly ambitious goals with some urgency.

1. Toward a New Understanding of Information Propagation and Mobilization

At the center of this report is a new framework for understanding gray zone IOs, the *propagation-mobilization framework*. Though the contours of the propagation-mobilization framework may seem simple, we believe its implications are profound. The framework holds that there are two lines of effort to gray zones operations: *propagation* (e.g., of communications, ideas, conspiracy theories, memes) and *mobilization*. Gray zone IOs, whether employed by adversaries or allies, can be understood as having one of two impacts on these lines of effort, creating *positive feedbacks* (amplifying effects) or *negative feedbacks* (suppressive effects). Not every gray zone IO has an impact on both propagation and mobilization, but gray zone IOs increasingly operate on both lines of effort simultaneously.

In this report, we examine how IOs are employed in gray zone competition to advance propagation and mobilization. In doing so, we employ an evolutionary framework that focuses on the IOs employed rather than on the actors employing them. The evolutionary framework has great explanatory potential in the social sciences, and for disinformation specifically. Coupled with this report's propagation-mobilization framework, evolutionary theory can illuminate the kind of IOs we will confront in the future.

The first benefit of the propagation-mobilization framework is that it avoids the information-disinformation binary that often dominates these discussions. We do not seek to avoid this binary because we possess a postmodern skepticism of truth. Rather, there are three reasons we believe the information-disinformation binary can be unhelpful to analyzing gray zone IOs. First, IOs can be significant even if they are true, and indeed, gray zone IOs have long included elements of truth. This can be said, for example, about the IOs historically employed by the United States. Analyzing the Central Intelligence Agency's information operations in the immediate wake of World War II, Thomas Rid notes that they employed a "blend of covert truthful revelations, forgeries, and outright subversion."[9] Second, even if an IO is true, it can at the same time be misleading. Disproportionate attention provided to certain factual incidents—for example, overemphasis on crimes committed by certain ethnic groups, or on adverse effects of certain vaccines—can conjure in the audience a feeling of ominous trends that may not reflect reality. And third, focusing solely on disinformation means that one will miss relevant evolutionary IOs that, while unrelated to disinformation in themselves, are *highly relevant* to the future of disinformation propagation. In other words, IOs are not unidirectional: disinformation actors do not simply learn from and copy other nefarious actors. Rather, IOs generated by "legitimate" actors may be coopted and evolved by nefarious ones. Anyone studying disinformation solely through the lens of disinformation-related IOs risks becoming blindsided to the evolutionary potential of non-disinformation IOs to be used by disinformation actors.

Another important reason to avoid the information-disinformation binary is truth decay in the mainstream media environment. Often the lines between information and disinformation are too brightly drawn by observers. Truth decay is determined by multiple factors in the information sphere, including the rush to publish, the push toward simplified clickbait, societal polarization (which increasingly extends also to journalists), and a social media environment in which the popularity of our every thought or viewpoint is immediately known. Mainstream media is often perceived as taking sides in cultural conflicts rather than representing objective truth. A vulnerability to adversary IOs exists when an audience perceives that those IOs better reflect the reality it experiences than does the mainstream information sphere. *If the mainstream information sphere loses credibility, it will lack counter-propagation power*.

A second benefit of the propagation-mobilization framework is that, through its emphasis on tactics over actors, the framework will help to avoid strategic surprise. Current frameworks tend to be actor-centric, a dynamic that can produce blind spots. For example, the January 6 attack on the U.S. Capitol surprised authorities, but should have been more foreseeable. Multiple mobilizations occurred from 2020-21 in the United States. In sequential order, the most important mass mobilizations during the period prior to the "stolen election" mobilization were: 1) anti-lockdown protests, 2) a pro-racial justice mobilization, and 3) a separate mobilization by militant anti-fascist and anarchist activists, particularly in the Pacific Northwest. The tactics employed on January 6 were not foreseeable through a framework focused narrowly on actors who mobilized around the notion of a stolen election, *but the likelihood of those events could be discerned by examining strategic evolutions across all four of these mobilizations*. For example, the mobilization strategies of massing to overwhelm authorities and shutting down buildings symbolic of political power could be discerned in all three of the previous mobilizations. Future mobilizations leveraged to subvert democratic systems can be better predicted and prevented through this report's framework.

A third benefit we foresee from this report's framework is that it can enable more precise identification not just of adversaries' use of emerging technologies in the gray zone but also the relevant signs that certain IOs are growing in significance. For example, several small-scale but relatively violent protests directly preceded the January 6 attack on the U.S. Capitol. These were conducted by groups such as the Proud Boys, which leveraged the notion of a stolen election to amplify, promote, and direct violence in these small-scale "seed" events, which showcased mobilization features from the previous three 2020 mobilizations. In particular, they showcased the shift to street violence

during the evening (dark) hours of the protests, skirmishes by the more aggressive participants, and vandalism of perceived opponents' property. *This highlights how groups' tendencies to replicate selected (useful) strategies across disparate mobilizations provides a road map for prevention and response planning.* Thus, this report's framework can empower democratic actors to select strategies and corresponding IOs that will yield the greatest return on investment over time.

The fourth benefit relates to strategic deployment of complementary capabilities. The propagation-mobilization framework allows for clearer categorization of the strategic purpose of various emerging technologies in the gray zone. Its categorization of gray zone IOs into those that will have positive or negative feedbacks on propagation and mobilization can enable the development of comprehensive strategies where each capability supports all other elements.

With the advantages we discern from this framework in mind, we now outline how the propagation and mobilization elements of gray zone IOs came to be more tightly wound with one another than ever before.

The Technological Change: The World of the Social Web. In the information sphere, technology has allowed ever greater dissemination of information and messaging. Recent developments in the digital sphere are no less seismic than was Johannes Gutenberg's invention of the printing press. Indeed, the internet itself has undergone two different revolutions in the past three decades.

The internet as it exists today is a far cry from where it stood in the 1990s. The first iteration of the internet, Web 1.0—the "read-only" internet—was characterized by static webpages that could be read but offered little to no interactivity. Around the turn of the century, Web 2.0, or the "read-write" web, emerged. This iteration allowed users to create blogs, post multimedia content (e.g., audio recordings or videos), and engage more easily with content on webpages. Web 2.0 offered greater interactivity but did not change the average internet user into a content producer. The social web turned this dynamic on its head. On sites in the social web (e.g., Facebook, Twitter, YouTube), users were no longer primarily consumers of someone else's material but were put in the position of being content producers themselves.[10]

Alongside the web's evolution, internet adoption grew globally, as did adoption of social media in particular. For example, Facebook had 608 million monthly users at the end of 2010. By the end of 2014, that number had soared to nearly 1.4 billion, and it has by now reached nearly 3 billion.[11] Thomas Rid notes how the changed technological environment transformed information operations. After tracing three preceding waves of disinformation, Rid writes that "the fourth wave of disinformation slowly built and crested in the mid-2010s.... The old art of slow-moving, highly skilled, close-range, labor-intensive psychological influence had turned high-tempo, low-skilled, remote, and disjointed."[12] It is this quick tempo of IOs empowered by technological changes that erodes the distinction between propagation and mobilization in the IO sphere. We illustrate this through the "virtual plotter" model employed by Daesh (also known as the Islamic State or ISIS), which represented a successful gray zone IO technique by a non-state actor.

Daesh and the Virtual Plotter Model. Though it is difficult to measure, most experts believe that radicalization to violent extremism is occurring faster than ever before (e.g., the time between an individual beginning to explore violent extremist ideas or identities and acting on their behalf is compressed). Social media, with its frenetic pace of communications and the social bonds it fosters, can create an environment where extremist groups more quickly influence people's identity formation in an extremist direction and drive them to action. Put differently, *the distinction between propagation of, and mobilization in service of, violent extremist ideas has become less pronounced*. Daesh's online activities demonstrate this.

In addition to using social media to help mobilize record numbers of foreign fighters to Syria during the country's civil war, Daesh engineered a process by which its operatives could directly guide lone attackers, playing an intimate role in the conceptualization, target selection, timing, and execution of attacks. Essentially, operatives in Daesh's external operations division coordinated attacks online with supporters across the globe, most of whom never personally met the Daesh operatives they conspired with. Virtual plotters thus could offer operatives the same services once provided by physical networks. The model helped transform lone attackers who relied heavily on the internet from the bungling wannabes they once were into something more dangerous.[13] Further, the virtual plotter model created a process whereby propagation and mobilization occurred through the same mechanism. This stood in stark contrast with earlier jihadist propaganda, which would put out calls for violence and hope that these calls would be followed without the groups having any real way of ensuring that people would take up their calls for action.

The experience of the first Daesh virtual plotter to gain international recognition, British hacker-turned-terrorist Junaid Hussain, illustrates how this model wed propagation to mobilization:

May 2015

- Hussain encouraged Elton Simpson and Nadir Soofi to attack the "Jihad Watch Muhammad Art Exhibit and Cartoon Contest" held in Garland, Texas. Simpson and Soofi arrived at the venue and opened fire but were quickly killed by an alert security officer.[14]
- Hussain was in contact with Munir Abdulkader, a 22-year-old from West Chester, Ohio. He encouraged Abdulkader to launch an attack against U.S. military and law enforcement personnel. Authorities arrested Abdulkader after he purchased an AK-47 to further this plot.[15]
- A 17-year-old with links to Hussain was arrested in Melbourne, Australia for plotting a Mother's Day massacre. Hussain provided the teen with bombmaking instructions and encouraged him to launch an attack in Melbourne.[16]

June 2015

- Hussain communicated with Usaamah Abdullah Rahim, a Daesh sympathizer who was killed while attacking a police officer and FBI agent in Roslindale, Massachusetts. An investigation following the attack revealed that Hussain initially encouraged Rahim and two co-conspirators to attack Pamela Geller, who had organized the Garland art contest.[17]
- Justin Nojan Sullivan, a 19-year old from Morganton, North Carolina, conspired with Hussain to plan a mass shooting that would be claimed in Daesh's name. Sullivan was caught by the FBI before he could carry out the attack. But in the weeks before the attack, Sullivan succeeded in murdering a neighbor.[18]
- Hussain communicated with Fareed Mumuni and Munther Omar Saleh, members of a small Daesh cell in New York and New Jersey. Hussain encouraged Saleh to conduct a suicide bombing against law enforcement officers, and Mumuni stabbed an FBI agent who was executing a search warrant at his residence.[19]
- Hussain recruited Ardit Ferizi, a Daesh sympathizer living in Malaysia, to hack into the server for an Illinois company and release personally identifiable information on around 1,300 U.S. military or government personnel who had shopped there. Daesh subsequently released this information on Twitter as a list of targets for militants in the United States.[20]

July 2015

- Hussain conspired with Junead Khan, who intended to attack U.S. military personnel in Britain. Hussain gave Khan bombmaking instructions and tactical suggestions. Khan was arrested prior to carrying out his attack.[21]

August 2015

- Zunaid Hussain, a doorman in Birmingham (U.K.), planned to detonate a bomb along the tracks of a rail line between Birmingham and London. Hussain reportedly communicated with Junaid Hussain over Twitter and Kik, another messaging platform.

Other examples of how the virtual plotter model wedded propagation to mobilization abound. Rachid Kassim, a French social worker turned jihadist, travelled to Syria to join Daesh in 2015. Like Junaid Hussain, he established a noteworthy social media presence, using his ability to speak both French and Arabic to connect with aspiring jihadists in his home country.[22] Kassim ran a popular Telegram channel, Sabre de Lumière (Sword of Light), in which he called for attacks in European countries and distributed "hit lists" of high-profile individuals.[23] He also engaged one-on-one with aspiring operatives, assisting them in carrying out attacks. Prior to his death in a July 2017 U.S. airstrike, Kassim was involved in numerous plots, including the following:

June 2016

- French authorities believe Kassim was in contact with Larossi Abballa, a 25-year-old French jihadist who murdered a police captain and his partner in Magnanville, France.[24] After slaying the couple, Abballa menaced their three-year-old child. He streamed this on Facebook Live, saying: "I don't know yet what I'm going to do with him."

July 2016

- Kassim was in contact via Telegram with Adel Kermiche and Abdel Malik Nabil Petitjean, who slit the throat of an elderly priest during services at a church in St. Ètienne-du-Rouvray. Authorities believe Kassim introduced the two operatives, who lived over 400 miles apart and first met in person shortly before the attack. Kassim took over Kermiche's Telegram account after he was killed by police, one indication of his importance to the attackers.[25]

September 2016

- Kassim was in contact with a 15-year-old French boy who planned to carry out a knife attack in Paris.[26]

October 2016

- Kassim was in contact with an 18-year-old who was arrested in Clichy-la-Garenne (Hauts-de-Seine) for plotting an attack.[27]
- Kassim was in contact via Telegram with a young couple in Noisy-le-Sec who were planning an attack. Authorities arrested them after determining that their attack was imminent.[28]

In addition to his role in these plots, Kassim succeeded in bringing disparate individuals together to form cells (as he seemingly did for the attackers in the aforementioned St. Ètienne-du-Rouvray church attack). In September 2016, French authorities arrested a group of female terrorists who tried to set off a car bomb near Paris's Notre Dame Cathedral. One of them stabbed an officer outside the Boussy-Saint-Antoine rail station as authorities made the arrest.[29] Before the attempted attack, none of the women had had any type of relationship with one another. Instead, they were brought together solely by Kassim. In connecting the women, Kassim merged two different

lines of terrorist effort in two different parts of France based on one operative's reluctance to carry out a suicide operation. Sarah Hervouët, a 23-year-old convert to Islam who was planning an attack in the southeastern French commune of Cogolin, had been communicating with Kassim over Telegram. Acting on Kassim's orders, Hervouët drafted her will, wrote farewell letters to relatives, and made a video proclaiming her allegiance to Daesh. But she lost her appetite for this "suicide-by-police" attack. So Kassim connected her with two other women preparing to carry out an attack in Paris instead.[30] Though the women failed to carry out the dramatic attack that Kassim hoped for, the Notre Dame case demonstrates the speed, agility, and adaptability of the virtual plotter model, and how it weds propagation to mobilization.

Pairing propagation and mobilization is even easier when, unlike in Daesh's virtual plotter model, the IO is not attempting to mobilize the target to do something illegal, in which case the possibility of legal penalties may serve as a deterrent. In recent years, adversarial IOs targeting the United States and Canada have tried to mobilize the target audience in multiple ways, including mobilizing to activities that are both legal (e.g., protests) and illegal (e.g., carrying out attacks, looting).

2. What Is Gray Zone Competition?

> *"This is another type of war, new in its intensity, ancient in its origin — war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him." -- John F. Kennedy*

The concepts of peace and war typically connote a binary condition—a white or black distinction. However, in the twenty-first century, interstate conflict is more likely to take the form of gray zone competition rather than outright war. The gray zone is the space between peace and major armed conflict or war. As its name implies, there can be multiple shades of gray. The gray zone is thus a spectrum between the two polar opposites, with the peaceful or diplomatic competition between states at one end of the spectrum and open, violent conflict between states at the other end. Many historical events since the end of World War II can be understood as residing along this spectrum, in the form of interstate competition that does not meet the threshold of open warfare. Such events can be termed *gray zone competition*. Gray zone competition can be seen in clandestine activities like intelligence collection, covert operations, and information operations). IOs, sometimes also called information warfare, refer to "the strategic use of technological, operational, and psychological resources to disrupt the enemy's informational capacities and protect friendly forces."[31] Such operations have been highly effective gray zone tools.

2.1 Introduction to the Gray Zone Environment

The gray zone presents significant security challenges for states, as activities in the gray zone can be hard to detect, define, and attribute. States must define for themselves what meets the threshold for an act of war. Competitors try to undermine a state's interests while staying below this threshold. Complicating matters further, the gray zone is notoriously difficult to define.

The gray zone is not a new space. Irregular warfare, low-intensity conflict, and asymmetric warfare have all preceded coinage of the *gray zone competition* concept. As far back as 1962, President John F. Kennedy described one aspect of what would now be called the gray zone, saying: "This is another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him."[32]

The gray zone possesses several unique characteristics. As Philip Kapusta describes it, the gray zone is "characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant

policy and legal frameworks."[33] The ambiguous nature of the gray zone creates challenges that do not exist in traditional decision-making models. The opacity of the gray zone allows both rival state actors and non-state actors to produce their own challenges to a state. Rival states and non-state actors can collaborate and work against a shared competitor, including via proxy relationships, which can create challenges in attributing any given gray zone activity to a single actor.

Gray zone challenges also depend on the perspective of the actor. As Kapusta points out, Russian activity in Ukraine may be a lower priority issue for Canada or the United States, one that might only merit economic sanctions, but it would be a top-priority issue for Russia if Western countries intervened. Miscalculation over such an issue could result in an unexpected escalation.[34]

One term sometimes associated with gray zone competition is *irregular warfare*. This term is defined rather broadly by the U.S.'s joint doctrine as "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations." But as Sandor Fabian notes, numerous "more specific conceptualizations" of the term have been advanced by scholars and practitioners alike.[35] Another term associated with the gray zone is *hybrid warfare*, which NATO has defined as "a wide range of overt and covert military, paramilitary, and civilian measures employed in a highly integrated design."[36] Thus, hybrid warfare can augment the deployment of conventional armies with non-conventional activities like covert operations or guerilla warfare. There is debate among scholars regarding whether hybrid warfare and gray zone competition are interchangeable terms. For David Carment and Dani Belo, hybrid warfare is a strictly tactical concept while gray zone competition represents a strategic concept. Hybrid warfare can be one form of gray zone competition, but hybrid warfare does not have to be present in an adversary's gray zone repertoire.[37] Some, like Jean-Christophe Boucher, disagree with this characterization and argue that hybrid warfare is in fact synonymous with gray zone competition.[38]

Beyond the definitional challenges, the amorphous and ever-changing character of gray zone competition presents challenges for effectively planning for, and responding to, adversarial activities. According to one U.S. Army War College report, gray zone competition is "hard to classify, hard to conceptualize, hard to plan against, and therefore, very hard to counter."[39] For liberal democracies, the gray zone can be particularly challenging when trying to counter or compete with authoritarian states like Russia, China, and Iran, which regularly employ influence operations, manipulation, and outright intimidation that fall well short of the threshold for war to achieve strategic gain. Gray zone tactics include the exploitation of divisions and destabilizing levers within a state or a strategic ally of a state. Such exploitation aims to produce the political outcomes desired by the threat actor. For example, a rival state can focus on enabling internal resistance movements or exacerbating underlying conditions to disrupt the status quo with the aim of toppling a government.[40]

Gray zone activities seek to alter the competitive environment such that the target does not perceive the change until it is too late. This phenomenon has been compared to the "boiling frog" fable, wherein a frog placed in boiling water would immediately jump out, while a frog placed in tepid water will not jump out as the temperature is slowly raised until it boils alive. Similarly, sudden upheavals in the international environment may prompt a swift response from world powers, but slow and barely perceptible changes can acclimate those same states to a new normal. In short, a clear and present danger will likely become a major priority to be immediately addressed, while multiple smaller nuisances are weighed amid competing priorities, allowing them to be put on the backburner until the strategic environment has dramatically changed, one barely perceptible step after another.[41]

One example of such gray zone competition can be seen in Russia's activities vis-a-vis Europe. The use of information operations aimed at undermining political institutions, coercive energy deals that exploit European reliance on Russia, military demonstrations along Russia's borders, and infiltration of disputed territory all highlight how

Russia uses IOs and seeks to compete in the gray zone.[42] Russian activities in Georgia, Crimea, and Ukraine's Donbas region all employ political, military, and economic activities that not only fall short of the threshold of war but are hard to properly attribute to the Kremlin.[43] As Russia has increased its activity in Ukraine, so too did the Kremlin increase its manipulation of energy resources, subsidization of pro-Russian media, interference in the Ukrainian electoral process, and the ambiguous and disinformation-laden deployment of Russian soldiers to Crimea. These soldiers deployed wearing generic green uniforms with no identifiable markings denoting the country they belonged to, introducing plausible deniability for Russia and prompting the soldiers to be referred to as "Little Green Men." These activities were made even more ambiguous by concerted information operations aimed at buying time for Russia to solidify its influence in the Ukraine, making information operations a critical component of gray zone competition.[44]

2.2 Information Operations in the Gray Zone Context

Information operations serve as a valuable tool for gray zone competition. IOs can exploit an adversary's internal vulnerabilities, such as societal divisions or political trends, through the dissemination of propaganda or other information that compromises a target in order to acquire a competitive advantage.[45] While IOs are not new, the modern information environment has provided new means for IOs to be employed, such as exploiting the viral nature of social media to reach unprecedented numbers of people, enabling what some have called a "firehose of falsehoods" stemming from rapid creation of false and easily shareable material.[46]

Information operations target the civilian population, making influence on a target population more relevant than ever. This notion of influencing a population is virtually timeless, as it is discussed at length in Sun Tzu's *Art of War*. Thousands of years later, World War I-era general officer Giulio Douhet put forth a theory of breaking a civilian population's morale, suggesting that the direct use of bomber aircraft against adversary populations could be a way to ensure victory on the battlefield.

Some modern IOs deployed by adversarial countries like Russia use social media propaganda, state-run news agencies, automation software, and fake online personas to amplify their chosen narratives. Russia's actions have focused on influencing European elections, distracting attention from Russian activities, and sowing confusion. In the words of Russian General Valery Gerasimov, "long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[47] Similarly, the People's Republic of China has used IO as a way of controlling the narrative around its Belt and Road Initiative to shape perceptions of the project as a tool of global peace rather than an effort to gain a strategic competitive advantage.[48]

Information operations also enable non-state actors to conduct gray zone provocation. For example, both al-Qaeda and Daesh have conducted IOs that spread their propaganda online, attack Western cultural values, and recruit. Internet forums, social media sites, and encrypted communications platforms have all served as key parts of these IOs, allowing al-Qaeda and Daesh to spread their propaganda, celebrate attacks, and recruit or inspire new members and attackers. Such efforts reflect that gray zone competition is not limited to states. Organized non-state actors can reach larger audiences by adopting modern technologies and adapting the information operations used by states to their own purposes.[49]

2.3 Gray Zone Information Operation Targets

Both state and non-state actors engaged in information operations against a target aim to shape the information environment in a particular way, often to distort the perceptions of a target audience toward a certain end. For example, by making a population have a more favorable view toward the actor, by exploiting divisions between

two or more groups, or by turning a population against a target state or political entity, a rival state can pursue a competitive advantage and/or achieve their end, typically a desired political outcome.[50] This can be done by amplifying narratives that align with the actors' goals, undermining or suppressing narratives that do not align with these goals, or influencing opinion to destabilize or interfere with an adversary's internal politics. To do this, actors rely on psychological biases inherent in the target audience, social and political structures within a society, the means by which information traverses through the information environment, and emerging technologies.

The demographic characteristics of a populace can be exploited by information operations. A U.S. Army manual on the conduct of IOs identifies factors like age, gender, education, literacy, ethnic composition, unemployment rates, and languages spoken, among others, as characteristics to be studied by IO officers. These factors impact how information transmits through the target environment and how it may be received by a target population.[51] An adversary could deploy IOs that seek to exploit these characteristics in ways that will destabilize a target.

Similarly, a state's social structures offer means that can be exploited by IOs. These include political, religious, and cultural beliefs, affiliation, and narratives.[52] State actors like Russia, China, Iran, and Saudi Arabia have all used divisive political topics to target divisions in the United States and Europe through "fake news" and social media bot accounts, which will be discussed in detail later.[53]

A state's media and information environment also shape the ways in which IOs can be conducted to reach a target audience in furtherance of an actor's gray zone ends.[54] Characteristics of this environment can include traditional print media, mainstream media (such as cable news channels), new and alternative media (such as newsletters or news websites), and social media. While discussed in more detail in the next section, actors can craft IOs that exploit a particular medium or multiple media formats to reach a tailored or a broad audience.

One way in which information operations are tailored to a target audience is through the creation of a strategic narrative of an antagonistic nature. Such narratives allow actors to create "a shared meaning of the past, present, and future" to influence behaviors both at home and abroad. This, for example, might entail a shared cultural tradition or origin story, like those found in religions that ground members in a shared starting point and purpose. While strategic narratives can tell a convincing story, a narrative used antagonistically can pull together a compelling story through misinformation, oversimplification, or even manipulated or intentionally falsified information that offers a distorted view of reality.[55] Given the complex nature of the world, a compelling narrative that allows otherwise chaotic or seemingly random events to make sense in the mind of the consumer is a powerful psychological tool. This tool can be deployed by a government communicating with its population, by malicious actors like hostile states or non-state actors, or by parties attempting to influence political discourse in support of their cause or agenda.

While the media environment was once more centralized, information and communications technology (ICTs) have rapidly evolved to enable broader content creation, producing fragmentation in the dissemination of information. Actors conducting IOs have taken advantage of this to create what scholars have termed situations of *implausible deniability*. Where plausible deniability seeks to enable secrecy of covert action, implausible deniability seeks to sow confusion by polluting the information environment in such a way that the public can no longer determine fact from fiction. This allows a state or non-state actor to gain a competitive advantage in the gray zone while its adversary struggles to determine what is happening. As one Russian practitioner of this approach suggested, the goal of implausible deniability is "to generate a situation where it is unclear whether a state of war exists—and if it does, who is a combatant and who is not."[56]

While IOs have previously sought to interfere in various countries' internal politics, the internet allows for organic amplification of IO efforts. These technologies allow for interference in elections, inciting and mobilizing individuals to violence, and undermining the legitimacy of democratic institutions, all at a distance and at a scale that can reach

millions of people with a single social media post. And newer technologies provide new ways of influencing a population. Deepfakes, artificial intelligence-produced videos, are one such method. Similarly, cheapfakes, poorly altered source material aimed at changing or implying something that is untrue, are another method of influence. While deepfakes have yet to reach the threshold of being highly impactful (though this dynamic appears to be changing rapidly), cheapfakes have already deceived audiences in ways that amplify false narratives.[57] Further, the very existence of these technologies enables a "liar's dividend," in which the existence of fake news, deepfakes, or other manipulated content can be leveraged to deny or write off documented bad behavior. A controversial remark or scandal can be denied or called into question by claiming that it is nothing more than manipulated or "fake news."[58]

As awareness of the threat of IOs increases, states, companies, and non-governmental organizations have placed greater focus on understanding the issue, but the means of carrying out IOs continues to evolve rapidly. In mid-2021, Facebook shared research into threat actors' use of the platform to carry out what the company termed "Coordinated Inauthentic Behavior" (CIB). As actors gain more experience with social media IOs, Facebook researchers noted a shift toward targeted efforts aimed at small communities. Actors are going to greater lengths to involve real people, as opposed to just falsified personas or automated accounts, in their IOs in an effort to lend an air of legitimacy to the operation. Actors are also diversifying to numerous platforms, including non-mainstream services such as Gab and Parler, to avoid detection and deplatforming efforts. Facebook researchers also noted that actors used "perception hacking," an IO tactic that exploits concerns and fears *about IO itself* to sow doubt and distrust (for example, in electoral systems).[59] Perception hacking takes advantage of the fact that when citizens no longer know what to believe, or when the amount of effort it takes to learn the truth about current events grows significantly, people disengage. Perception hacking can thus foster a sense of apathy. Voters who are primed to expect an IO targeting elections may question the validity of the election results if their candidate loses. The result is an erosion of the so-called trinity of trusts: trust in democracy, authority, and one's fellow citizens.[60]

3. The Gray Zone Information Context

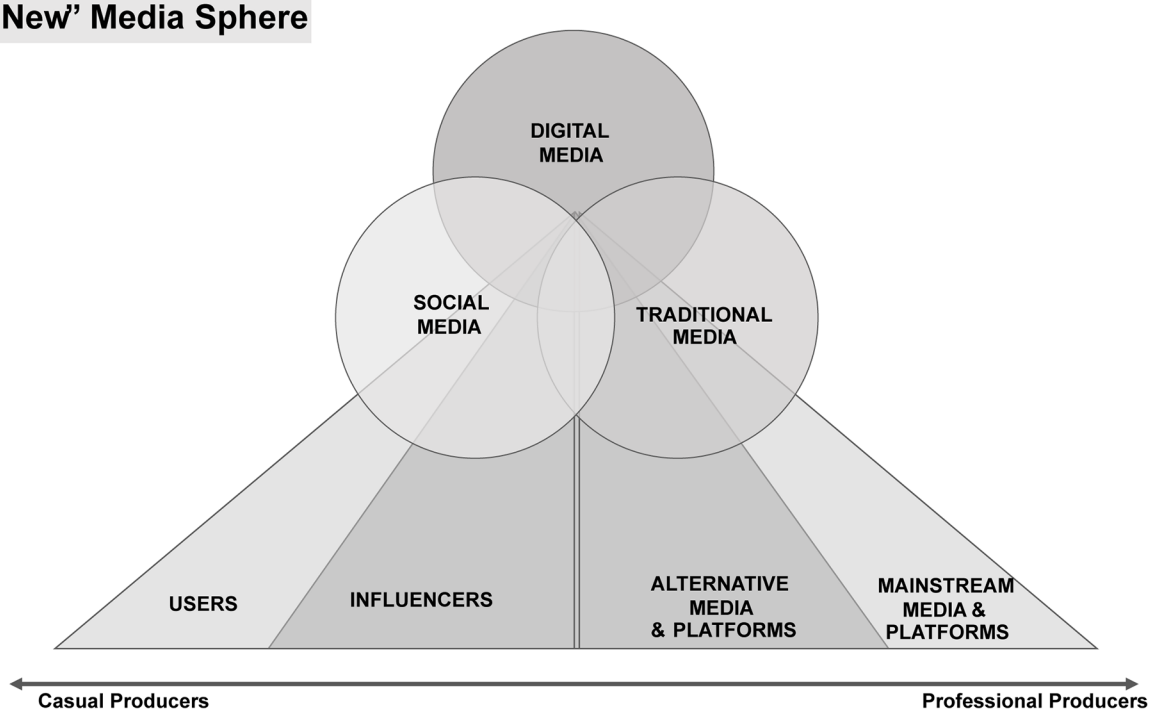
To understand the development and deployment of these gray zone IOs, it is necessary to describe the "new" media ecosystem—inclusive of technology, people, practices, and culture—within which they form and evolve. Today's media ecosystem is composed of a set of interrelated technologies—traditional, digital, and social media—available for use by participants who may act in various capacities as sources, producers, or consumers of information, sometimes taking on all three roles.

3.1 The "New" Media Ecosystem

The contemporary media ecosystem has undergone significant shifts from prior eras when "the media" consisted of a limited set of information technologies and sources controlled by professional and governmental institutions. These shifts are predicated on the development of new information and communication technologies over the last four decades, including the development of Web 2.0 and ultimately the social web, as discussed earlier in this report. Today's information environment vastly expands "the media" by conjoining digital media, social media, and traditional media technologies with multi-directional information sources both professional and casual, along with interactive participation on a global scale.[61] This shift has enabled broadened public, as well as institutional, access to participation in producing, consuming, and circulating information. It has also reduced informational guardrails rooted in professional ethics, democratic values, and factual norms. As such, this "new" media (and information) ecosystem has enabled gray zone information operations at a speed and volume previously unimaginable, and with material effects on politics, social polarization, and violence.

Today's information environment is characterized by increasing complexity of the new media ecosystem in terms of technologies, media sources, and audiences. Its growth and development also exhibit divergent tendencies (in technological, media, and audience layers) toward both consolidation and fragmentation.[62] The tendency toward consolidation is most prominently seen in technological development and commercial ownership. For example, Facebook's incorporation of Instagram, WhatsApp, and other technologies developed by smaller startups is a strategy to consolidate multiple types of services to engage a variety of user interests and ensure the company's commercial dominance. Conversely, fragmentation can also be seen in technological development and commercial ownership. For example, Twitter-like social media platforms Gab, Parler, and Gettr formed in response to conservative beliefs about left-wing bias in moderation on mainstream social media platforms. This ongoing tension between consolidation and fragmentation has implications for shaping information flows through the practices of users, platforms, and other media and information sources.

The "New" Media Sphere



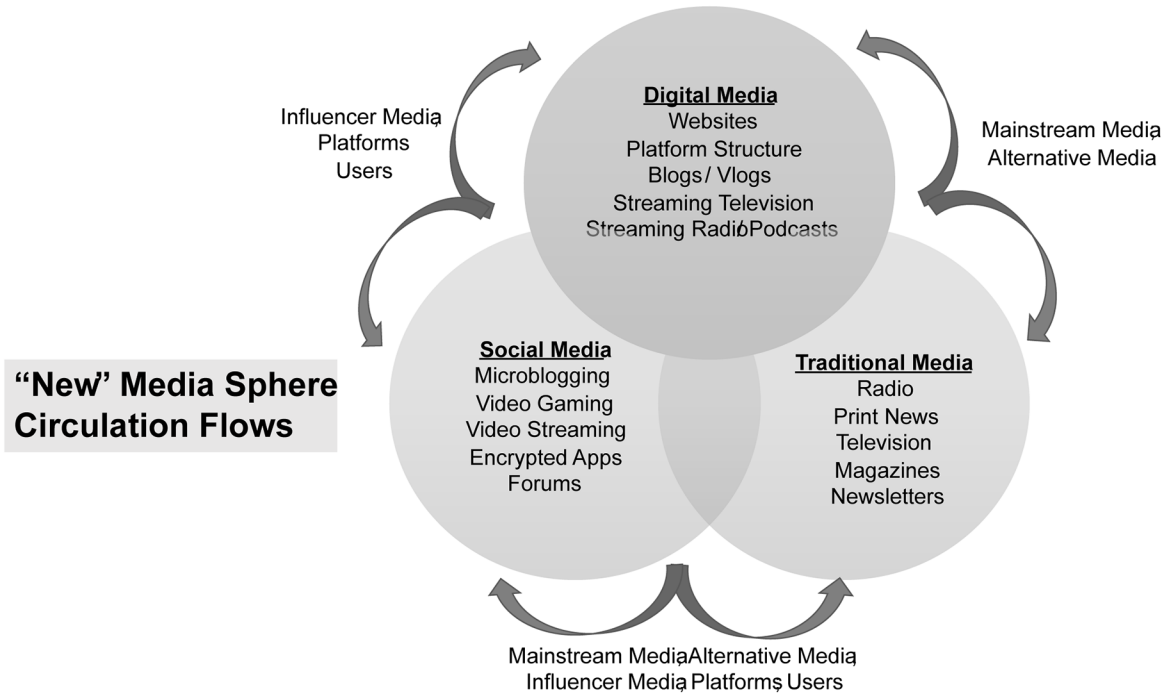
3.2 Technological Arenas of the New Media Ecosystem

The technological arenas that comprise the new media ecosystem are traditional media, digital media, and social media. The technologies used in each arena act as delivery mechanisms for informational content, thus mediating people's access to and uptake of information. The *affordances* (range of possible uses that dictate how an object should be used) of each technology shape how information is selected, stories and narratives are produced, and how the resulting products are presented. For example, the technical limitations of page width and bleed margins determine which fonts and lengths are used for textual headlines in print news, which also determines how headlines are written and edited.

Traditional media (e.g., print media, radio, televisual media, and film) each have relatively stable affordances that require specialist training in media production and access to equipment and infrastructures controlled by professional institutions. These media, often considered public media and infrastructures, are highly regulated and have strong professional standards and norms associated with their processes and practices of information production and dissemination. These standards are well known with respect to the journalistic practices of news media, but they also include the heavily regulated and professionalized standards for televisual programming, the film industry, and the radio industry. Whether audiences are interested in news, entertainment, education, or other varieties of information, they are largely passive consumers of the informational products of these traditional forms of media. The audience passivity and professionalized control associated with traditional media technologies, however, are primary features dispensed with in the technologies and forms of "new" (e.g., digital and social) media, which are designed to favor interactivity and "democratized" open access to information.

Digital media (e.g., the internet, streaming platforms, and smart, web, and cloud-based technologies) have broadly ranging affordances that remain in flux as they are dependent on continued technological development. These media, unlike traditional media, cross international borders, are used for business as well as information and entertainment, and are interconnected globally, thus posing a higher degree of regulatory complexity. They tend to be more loosely regulated by governments, and often companies' terms of service and industry standards provide the primary regulatory structures. Digital media are considered private media, though debates over their regulation and including them in public media and infrastructure are ongoing. While digital media may require technical specialization to navigate use of affordances, particularly for infrastructural systems and coding/development, digital technologies have trended toward ease of use for average people. So, while digital media specialization may be acquired through education and traditional modes of professionalization, it is also accessible to any person who wants to learn about the technologies, coding, web development, etc., as well as through user-friendly devices and user interfaces that have enabled widespread content production and dissemination by average users (e.g., blogging, vlogging, video streaming, and podcasting). Standards for information and content sharing—particularly on web-based digital media—have developed through lay use rather than through professional or ethical standards, and thus reflect cultural norms.

Social media (platforms and apps that function to interconnect and network people according to their social connections and interests) has highly specific affordances based on platform and app design, often dictated by a preferred medium for content (image, video, music) or combinations of such media typically available through microblogging functionalities. Image-based social platforms include Flickr and Instagram, video-based platforms include YouTube and Bitchute, and music-based platforms include Pandora and Spotify. Almost all social platforms include functionality for some inclusion of text, though text-based platforms often also enable the sharing of visual media (e.g., Facebook, Tumblr, Twitter). In addition, social media have long included "anonymous" platforms like Reddit, 4chan (and 2chan, 8Chan, 8kun), and other forum-based platforms. Like digital media, social media are private media with vast global reach. Affordances in the social media environment are highly platform/app specific, adaptable, and manipulable by all users. As a particularly user-friendly sector of digital media, social media technologies are designed to be intuitive to users, as well as built and developed with content production and dissemination capability as essential features for keeping users engaged. Social media, and digital media more generally, have enabled not only broadened access to information but have also increased by vast orders of magnitude the sources of information that circulate in the media ecosystem. Social and digital media have also provided avenues to monetize user-produced content and given rise to a new sector of the media production and information industry in the form of influencer marketing, a sector that has an increasingly tangible impact on socio-political information in the new media ecosystem.



Digital and social media have generated three primary characteristics of the new media ecosystem: 1) convergence, 2) interactivity, and 3) global "public" access to vast quantities of data. These three characteristics functionally increase the complexity of the media ecosystem and information environment with definite impacts on the practice and effectiveness of gray zone information operations. The first characteristic, *convergence*—a term prominently employed by Henry Jenkins—is generally understood as a technological process of consolidation, bringing together disparate technologies and capabilities into single device forms.[63] Media scholars, however, have argued that while convergence is easily seen in technological development, it is better understood as a cultural shift inclusive of technologies, media practices, human informational processing, and participatory engagement.[64] The second characteristic, *interactivity*, regards a shift from generally unidirectional information flows from institutions and professional media to multidirectional information flows enabling a variety of non-institutional and non-professional sources. Interactivity not only enables, but demands, participation in the information environment and media ecosystem in ways that change our understanding of authoritative information, leading to public contention and debates about facts and truth. The last characteristic, *global "public" access to vast quantities of data*, is a function of the access provided by digital media, particularly the internet. However, this characteristic functions in coordination with the first two characteristics—convergence and interactivity—to shape how people consume, digest, and derive meaning from information within this new media ecosystem.

Digital and social mediation also impact the workings of traditional media (print, television, and radio). The most apparent change has been to print media, with massive decreases in circulation in journalistic print media (newspapers and magazines). Other, perhaps more subtle, changes have occurred in television media and radio,

specifically in relation to digital streaming services, webcasting, podcasting, as well as blogs and video blogging (vlogs). To adapt to these changes, media companies have incorporated them into their services, running websites that house digital news in multiple formats as well as running multimodal media services across a range of platforms, from branded websites to social media and streaming services. Newer journalistic companies have also developed as "born digital" multimedia experiences. For example, *Vice Media*, dubbed "a poster child for new-media success" by *Fortune* magazine, started with a print magazine in 1994 but rapidly eschewed traditional media formats in favor of digital expansion.[65] The company now boasts *Vice* (News), *Vice Studios*, *Refinery 29*, *Pulse Films*, and *Motherboard* among its multiple brands. Other more subtle examples of the interactivity demanded of traditional media companies by digital mediation occur in relation to the development of social media norms with a particular focus on trends and virality. Now media companies source stories from social media trends and viral topics. Moreover, these stories reference details and "evidence" from social posts, in some cases creating feedback loops and in other cases spreading polluted information. For instance, Jenna Abrams was an Internet Research Agency-created account that served as a news influencer. Before Abrams's true origin was discovered, the account "was featured in articles written by Bustle, U.S. News and World Report, USA Today, several local Fox affiliates, InfoWars, BET, Yahoo Sports, Sky News, IJR, Breitbart, The Washington Post, Mashable, New York Daily News, Quartz, Dallas News, France24, HuffPost, The Daily Caller, The Telegraph, CNN, the BBC, Gizmodo, The Independent, The Daily Dot, The Observer, Business Insider, The National Post, Refinery29, The Times of India, BuzzFeed, The Daily Mail, The New York Times, and, of course, Russia Today and Sputnik."[66] A *Daily Beast* profile examining the outsize impact of the Abrams account noted that "many of these stories had nothing to do with Russia—or politics at all."[67]

Audiences react and respond to media companies directly and in real time via social media and digital platforms. They share stories and expand participation in those companies' online services, and even provide further content sourcing.

3.3 Information Sources

Along with the technological arenas of the new media ecosystem, it is essential to understand how sources of information are changing the information environment and contributing to gray zone information operations. The tension between consolidation and fragmentation, as well as the characteristics of convergence, interactivity, and global public access to vast quantities of data also impact how and where information is sourced. In prior eras, mainstream media was a primary and shared source of information for the majority of audiences. Alternative media existed—including subscription-based newsletters and magazines, as well as community and pirate radio stations—but each of these required specialized knowledge or association for access. They were also largely separated from mainstream media, with limited capacity to influence the normative information environment. In the new media ecosystem, mainstream media and alternative media remain sources of information, although their balance of interaction and capacity for influence has shifted substantially. The new media ecosystem also incorporates influencer media, platforms, and users as information sources. These sources and the information they spread now interact and inform each other in various ways that can be manipulated to the benefit of gray zone actors.

Mainstream media remains the primary source utilizing traditional media technologies and public communication infrastructures. As such, it is also the primary locus of industrial employment for media professionals (e.g., journalists, personalities, talk and radio show hosts, news presenters). The moniker "mainstream" indicates these media as being situated within and purveyors of normative—that is culturally, socially, and politically acceptable—discursive flows, even as those flows have, in the current ecosystem, developed clearly disparate strands of interpretation of information, events, and even facts. Mainstream sources have thus generally been considered reliable and fact-based information sources, particularly because they are subject to professional ethics and regulatory oversight. In

the new media ecosystem, however, the mainstream media have had to adapt to the shifts brought by digital and social media technologies. Most mainstream media sources now incorporate both traditional and "new" media publication and dissemination outlets. Newspapers have incorporated digital platforms and use social media to build interest in their "products." Similarly, televisual media and radio have incorporated websites and use social media to build online followings, but now also incorporate streaming media (e.g., video and sound clips from broadcasts, online-only streaming content, as well as podcasts and streaming radio shows). Moreover, mainstream media sources have turned to social media trends and viral content to source their own stories and news.[68] In addition, if the uptake of digital and social media as technologies and information gathering sites presents a form of fragmentation among mainstream media sources by pluralizing modes of access and engagement, consolidation is at play often through the consolidation of specific channels by media corporations. In this process, competition among media corporations is reduced as a limited number of large companies buy up smaller entities and channels (e.g., radio or local television stations or newspaper publications). Consolidation here provides a mechanism for potential control over messaging and story selection through these channels. In the context of political polarization, both fragmentation and consolidation in mainstream media can work to further delineate and strengthen disparate strands of interpretation and socio-political disagreement over facts and events, essentially reifying consensus within disparate strands while disrupting consensus between them.

Along with mainstream media's uptake of and interactivity with digital and social media, under the new media ecosystem it has also become more imbricated with alternative media. "Alternative" is a category judged against the normative "mainstream," and as such may change over time and in relation to sociopolitical and cultural shifts. For example, under the Trump presidency, multiple previously "alternative" media sources and channels were elevated to "mainstream" status, at least nominally, because the Trump administration categorized them as preferred media.[69] Alternative media may include professionally trained media personalities and workers, but it also includes "citizen journalists" and other informally or untrained sources, it is less heavily regulated (if at all), and it is not subject to professional ethics. Unlike mainstream media, alternative media sources include extremist, activist, and other politically motivated information sources that increasingly position themselves as "telling real truths" that the mainstream media ignores or covers up. Alternative media sources have made ample use of the new media ecosystem's technologies, and have often been early adopters of new information and communication technologies.[70] Early adoption, lack of regulation, and different organizational (or individual) goals have enabled alternative media sources to become agile in testing information strategies and tactics in relation to new media ecosystem technological developments.[71] Importantly, alternative media have been able to take on and participate in shaping the cultural ethos of digital and social media in ways that mainstream media have not due to ethical, professional, and economic considerations. This has led to a twinned development of industrial, corporatized alternative media (e.g., Vice Media, Mother Jones, One America News Network, Newsmax) alongside seemingly "grassroots" influencer alternative media (e.g, InfoWars, Joe Rogan Experience, Drudge Report, Young Turks).

Influencer media sources are a mainstay in the new media ecosystem. These sources highlight how digital and social media blend sales (advertising) with news (information) to persuade followers (audiences) through affectively charged forms of persuasion. The influencer business model formed after the shift to Web 2.0 technology, which made web development easier for average users. As blogging took off in the mid-2000s, companies realized that bloggers had begun amassing large, loyal readerships, and that those followings could be tapped as consumer markets through a digitized form of "word-of-mouth" advertising, including blogger reviews of their products. This enabled bloggers to monetize their output and incentivized them to build their own brands. Importantly, influencer marketing and later influencer social media as communicative forms trade on their capacity to build a sense of authenticity and trustworthiness in their follower-bases. This type of marketing relies on relational communicative frames that mobilize heuristic persuasion—or the promotion of reduced elaboration (critical thinking) in favor of

emotional response to make choices—rooted in the audience's affinity for and trust in the influencer. The higher level of affinity influencers have with their audience, the more likely followers are to see information that influencer shares as trustworthy, valuable, and meaningful.[72] Affective (emotion-based) reasoning has come to characterize online information-sharing cultural norms, helping to enable intensified information consumption practices like virality.[73] As social media developed, the influencer model has become increasingly ubiquitous, taking on a variety of forms based on the specific features (affordances) and cultures of popular platforms, shifting with platform audiences, and developing into a model in which influencers integrate their use of multiple platforms, known as *360 degree lifestyle branding*.[74] Influencers are curators of taste, culture, and information. They help reduce the "noise" of the digital space and provide their followers with easy access to preferred content, brands, and important news.

As influencer cultures and social media have developed, the influencer model was applied to new areas of information, particularly in news and politics. This is the site where alternative media and influencer culture converge, leveraging the growth of streaming technologies (e.g., podcasting or vlogging) to produce new media content and spread it broadly, often as part of a "culture wars" approach to shifting sociopolitical discourse and opinion.[75] These influencers style themselves as political commentators discussing their point of view and hosting discussions with other figures whom they deem important, thus mirroring mainstream news and radio discussion formats. Often these influencers are connected in networks and host each other on their shows, cross-marketing to their follower bases. For example, this media strategy has been used effectively by so-called "alt-right" and "alt-lite" digital and social media personalities (e.g., Richard Spencer, Mike Cernovich, Stephan Molyneux, Milo Yiannopoulos, Brittney Sellner, Lauren Southern) and alternative multi-media brands (e.g., Red Ice Media) focused on shifting political discourse around issues such as immigration or race and gender. This influencer strategy employed by the alt-right and alt-lite has been termed the *Alternative Influence Network* (AIN) by scholars studying media manipulation.[76] The AIN demonstrates how members were able to monetize their ideologically motivated sociocultural and political opinions to make careers out of driving political polarization.[77]

What is crucial about influencers as media sources in the context of gray zone information operations is that the model primes followers for mobilization in online and offline settings. Mobilization in this sense can mean simply buying the products suggested by the influencer, online mobilizations in support of the influencer (e.g., responding to challenges, promoting the influencer's brand, or attacking criticisms of the influencer), or offline mobilizations (e.g., public protest, electoral engagement) in response to the influencer's promotion of specific issues or ideas. Influencer models are premised on leveraging the affinities of followers who feel that the influencer is their friend (or like them) to motivate action. Given the massive growth in the trend and its incorporation of other sectors (politics and news), influencer marketing has proven to be a highly effective framework for utilizing affinity-based persuasion to mobilize users.[78] This is particularly pernicious when influencers spread polluted information, conspiracy theories, or extremist messaging. For example, research by the Center for Countering Digital Hate and Anti-Vax Watch (an alliance seeking to educate the public about the anti-vaccine industry) shows that up to 65% of COVID vaccine disinformation posted on major social media platforms from February 1 through March 16, 2021 originated from the accounts of twelve prominent anti-vaxx influencers.[79] Influencer campaigns—whether localized to target specific groups or globalized to target all potential user groups—seek to engage word-of-mouth, or in digital contexts the user-to-user spread of information, to amplify their message, brand, products, or ideas. This form of user engagement leverages networked interrelations created by digital and social media to employ individual users in their own capacities as media sources in the new media ecosystem.

Users serving as media sources is a hallmark of the new media ecosystem and a primary feature of Web 2.0 (and later) technologies. This capability is often framed positively, particularly by tech companies, as the democratization

of information, media, and technology.[80] However, the "liberation" of information and media has also promoted illiberal and anti-democratic trends. As media sources, users can now act as content producers, content disseminators and aggregators, and content consumers. Many users employ all these capacities regularly. These user capacities in the new media ecosystem are the primary driver of Jenkins's notion of cultural convergence (discussed above) as users bring various strands of information, symbols, and media together and create new, often unexpected meaning out of them, which can then spread globally to other users with wildly different frames of reference.

Users' capacity as content creators and media sources has continued to increase, becoming normalized as part of daily life, particularly through digital and social media's omnipresence tied to smart, wireless technologies. Statistical reports show that as of July 2021, there are 4.48 billion active social media users across all platforms (total users, not unique users). Moreover, 99% of users access social media from mobile phones, and the average user spends around 2 hours and 24 minutes on social media daily. There are now six social media platforms with 1 billion or more users, and 17 social media platforms with 300 million or more users, with Facebook owning four of the top six platforms and Chinese ownership of six of the top seventeen platforms.[81] These statistics highlight the importance of users as consumers, creators, and sources of information.

Platforms hold a unique space in the new media ecosystem, as they make up part of the infrastructure of digital and social media. A *platform* is a product that serves or enables the functioning of other products and services, and as such they exist at multiple layers in the new media ecosystem.[82] In the new media ecosystem this includes web and cloud hosting services (e.g., AWS, EPIK, GoDaddy), mobile services platforms (e.g., IOS, Android), publishing and content creation platforms (e.g., WordPress, Canva), social networking platforms (e.g., Facebook, Twitter, Instagram, Pinterest), and streaming platforms (e.g., SoundCloud, TikTok, YouTube). In some cases, as with Twitter and TikTok, platforms serve multiple purposes, including social networking, streaming, and content production. Typically, social media platforms argue that they are not publications precisely because it is their users, and not the platforms themselves, that are the producers and sharers of content.

However, recommender services and content moderation position these platforms as information sources in certain important ways, through aggregation on the one hand and through the gatekeeping of information on the other. Aggregation services include algorithmic recommendation systems tied to the popularity of content ("trending topics") or to the user's prior selections on the site ("suggested for you"). These recommender systems, powered by artificial intelligence/machine learning algorithms (which are not transparent, as they are held as proprietary information) curate sets of information from the massive amount of data and content on their sites. These algorithmically composed selections of content are then seamlessly provided to users as a value-added service. However, this value-added component is not only for users: It also benefits the platforms by keeping users on the platform for longer periods of time, exposing them to more advertisements, and thus increasing the platform's financial value.[83] The second mode through which platforms act as media sources is through content moderation: selecting which content is allowed to remain on the platform and which is not, and which content will circulate through recommender systems or have its circulation suppressed.

Consolidation and fragmentation as processes of the new media ecosystem work through interaction between and among these various sources. For example, some media sources have begun in the alternative space and utilized corporatization along with conglomeration as consolidation strategies to move into the mainstream while attempting to retain their public ethos as "alternative" media (e.g., Vice Media). Conversely, other sources market themselves as mainstream media while incorporating alternative and extremist content creators and influencers in their programming and publication. While influencer and user sources often rely on information from mainstream and alternative media sources as a basis for their content creation and brand development, mainstream and alternative

news sources invert this process by now looking to viral content and trends, often produced by influencer and user sources, to develop their own stories.[84] Further complicating source functions and the complexity of the new media sphere is the effect such interactivity has on information produced by various sources. Generally reputable media may provide polluted information and disreputable media may provide normative, fact-based information.[85] In both cases such inclusions may be oversights, intentional, related to differing views about what constitutes extreme positions, or driven by attempts to increase the monetization of content. But regardless of the underlying reason, they have effects on larger issues of trust in the media and polarization.[86]

3.4 Information Production and Interactivity

To better understand the new media ecosystem, scholars are exploring how people interact with information and media, as well as the ways new media shape informational affinities, change organizational structures, and produce new modes of communicative practice. In this frame, user behaviors—including the production of information (source), the sharing of information (agents of spread), and the consumption of information (audience)—are primary vectors of theorization and analysis. This section provides a brief discussion of research on the potential negative effects of technology in relation to social fragmentation and political polarization, and research on the potential effects of users' communicative adaptations to social media environments in relation to information production, sharing, and spread.

Common aspects of this research that have been taken up in discussions important to understanding information operations include studies and theorizations about the effects of digital and social media in relation to politics, polarization, media manipulation, and mis/disinformation. Conceptualizations of informational polarization, particularly the concepts of *filter bubbles* and *echo chambers* (discussed in detail below), have been prominent points of discussion. They are an attempt to analytically describe the processes of social fragmentation promoted by the new media ecosystem. However, when used as standalone analytic frames, such concepts may offer a limited view of the informational and relational processes extant in the new media ecosystem. Furthermore, as analytic frames, they do not account for the other aspects of the *convergence* equation: consolidation and global public access to vast quantities of data. Here the concept of context collapse (discussed in detail below) explores how users produce and share content differently in digital media contexts. This research suggests that simple increases in information diversity may not produce resulting social cohesion or political moderation.

Thus, while polarization is a major area of concern, it is only one salient effect of new media ecosystem information flows. Moreover, polarization and social fragmentation are not only produced because of digital and social mediation. They have been effects identified with mass media consumption since at least the eighteenth century.[87] A different picture of processes and potential threats emerges when the new media ecosystem—its technologies, sources, cultures, and norms—is viewed from broader, more fluid perspectives. An approach that incorporates the relations between localized activities and global effects may be obscured without a broader exploration of the ways ordinary, seemingly non-political, actions enable and enhance the effects of large-scale information operations.

3.5 Potential Negative Social Effects of the New Media Ecosystem

In the context of information, digital media, and sociopolitical polarization, research has taken up discussion of the negative social effects of antagonistic information frames combined with the fragmentation of information sources. From this research, concepts such as *filter bubbles* and *echo chambers* have become popular metaphors for describing political polarization and social fragmentation in relation to digital media technologies. Though no consensus definition of these terms currently exists, we can provide approximate definitions of both concepts.[88] *Filter bubbles*, a term coined by Eli Pariser, describes the potential for algorithmic filtering, specifically personalization algorithms

on social media platforms, to reduce the diversity of information and opinions to which individual users are exposed, thus amplifying the human tendency toward confirmation bias (seeking out information that confirms our existing opinions).[89] *Echo chambers*, in the digital context, refers to the potential for users to become segregated into narrow ideological or interest-based groups with the effect of increasing political polarization, social fragmentation, and extreme positions.[90] The concern is that filter bubbles and echo chambers work to limit information diversity, thereby reinforcing socio-political divisions and strife. In the context of gray zone information operations, such socio-political polarization is of high concern given its potential for exploitation.

As compelling as the concepts of filter bubbles and echo chambers may seem, empirical research has yet to demonstrate their existence, effects, and processes.[91] Moreover, the notion that digital and social media limit information access is contested: some research suggests that they increase rather than decrease information access.[92] Regardless, research on both sides of the debate over information limiting environments, while wide in scope, is limited in terms of usable findings. These limitations are rooted in variance between study designs, a lack of consistent measurements, a focus on measuring different behaviors and outcomes, as well as the difficulty of conducting studies on data at scale. These problems are exacerbated by a dearth of conceptual clarity in these terms.[93] Studies are beginning to identify and address these gaps, for instance by comparatively examining several major platforms to determine the different ways that algorithmic systems and social network relations on each platform impacts information consumption and bias. Findings suggest that different platforms have different effects—neutral, moderating, and partisan—on users' information consumption, suggesting that some platforms produce more information-limited environments than others.[94] Such studies highlight the complexity of understanding how information environments are shaped by technologies, sources, and users.

While a focus on the potential effects of technology is important, so too is a focus on the effects of user choice and relationships between users in an increasingly interconnected, networked environment where users act as consumers, sources, and agents of informational spread. When users act as sources and spread information, the way they frame and present what they are sharing is highly dependent on whom they imagine as their audience.[95] Research exploring users as source and audience in relation to the interactivity of social media technologies takes up a focus on the phenomena of *context collapse*, or the ways that "networked audiences" may preclude common offline communicative practices used to manage audience expectations through varieties of self-presentation.[96] Users make choices about what information to post, share, comment on, and potentially with whom they will share that information. Users' selections are often guided by whom they imagine their audience to be on a given platform, although their imagined audience and actual audience may or may not be consistent.[97] Over time, social media platforms have added technological enhancements such as filtering and groups to assist users in maintaining contextual boundaries in relation to the audience for their posts and shares. These technologies, however, are limited and platform-specific, as well as having to work against other intra- and inter-platform technological features, such as auto-recommendations within platforms and automatic cross-posting between platforms. Context collapse can have the effect of broadening an audience and increasing informational diversity. It may also pose new problems in terms of audience satisfaction with content, as differently oriented audiences may respond negatively to posts out of their context, activating "spirals of silence" or self-censorship if users perceive a topic will engender negative response.[98] Additional research has focused on how context collapse and volume of content impacts information consumption, specifically whether users experience "source blindness," essentially "users paying reduced attention to sources" of news.[99] This research helps us to better understand the spread of mis/disinformation. Overall, context collapse research highlights users' choices and ways that social relationships impact the sharing, spread, and consumption of information in the new media ecosystem. A particular focus of this research is how digital media produce new forms of relationality between users, and between users and technology, as a framework for better understanding and describing contemporary communicative practices.

Thus, while filter bubbles and echo chambers might be problematic and exploitable functions of the new media ecosystem, they are but one set of functions among an array of functions. Similarly, context collapse may contribute to more interactivity among a wider range of users but may also lead to either increased spread of mis/disinformation and self-censoring behaviors that work against the supposed benefits of information diversity. Moreover, context collapse, filter bubbles, and echo chambers are not all-encompassing, monolithic functions in terms of potential information weaponization.

Thus, information diversifying functions may not be solely beneficial, but may also have negative, potentially exploitable effects. And no matter how information limiting environments (filter bubbles and echo chambers) ultimately function, they do not function in isolation. Even highly partisan information environments must be reactive to the broader information sphere, media ecosystem, and real-world events to remain viable. Additionally, individuals and groups engaging in information limiting environments in one aspect (e.g., political news), may be exposed to wider diversity in other lines of information engagement and consumption, for instance through entertainment media. Thus, a broader conceptual and analytical frame is needed to explore how the new media ecosystem, its component players (e.g., sources, technologies) and its effects produce gray zone information operations.

3.6 Reconceptualizing Socio-Cultural Relations Through Information Circulation

To assess IOs that have been adopted in the new media ecosystem, and their evolution, utilizing more fluid conceptual and analytic frames is necessary. Theories of publics and media "spreadability" offer traction in exploring the complexity of the new media ecosystem through the interaction between its technologies, sources, practices, and effects. Publics as a conceptual and analytic frame attends to how people engage in public deliberation, form sociopolitical affinities and groups, as well as how such deliberation and group formation impacts politics and policy. Spreadability as a conceptual and analytic frame assesses how information and media move (circulate) between people and technologies, shape and are shaped by economic drivers, and have impacts on sociopolitical, economic, and cultural life.

Publics in a traditional political conception are "coherent groups acting with shared concerns and interests within the broader imagined community of the public sphere as part of democratic political processes."[100] In online spaces, coherent group structure and the typical foci common to traditional political conceptions of publics are limited due to digital cultural norms.[101] Two specific conceptualizations of publics in relation to media and information consumption better fit the nuances of online structures. Michael Warner conceives of publics as self-organized "space[s] of discourse," that function as a relationship among strangers, mediated by cultural forms and contingent upon historical context, which come together through "mere attention" (not agreement), and are thus "the social space created by the reflexive circulation of discourse."[102] This provides a way to understand online relational (e.g., socially networked) structures as publics that are formed through discursive association and as interactive through mediation by users (reflexive circulation). Lauren Berlant, building on Warner's approach, developed the notion of "intimate publics" to account for identity-based and categorical affiliation in discourse-based, consumption-driven publics.[103] Both conceptualizations are useful for exploring IOs that utilize online networks and the affordances of digital and social media to circulate information. The concept of intimate publics is particularly useful for understanding how media circulates and affinities form through grievance frameworks (e.g., racism, sexism/misogyny, class, nationalism, political affiliation).

Intimate publics, as Berlant defines them, refers to the formation of public-ness through the circulation of discourse where engaged individuals have an expectation "that the consumers of its particular stuff [discourses, texts, and commodities] already share a worldview and emotional knowledge that they have derived from a broadly common

historical experience," and a sense of shared oppression.[104] For example, this concept is useful in analyzing how anti-mask, anti-vaccine, and anti-lockdown narratives are linked in online discourses connecting communities interested in a disparate range of issues such as health and wellness, holistic and natural living, and patriotism and constitutional rights. It is a concept that is also useful for analyzing how these disparate strands come together in ways that have mobilized offline protests, have created deep-seated vaccine hesitancy and refusal, and sparked a burgeoning merchandising ("merch") business in so-called protest wear, including sarcastic anti-masker face masks.[105] In intimate publics, individuals feel the truth of a discourse rather than deliberating about its veracity. Attachments with a discourse may be positive or negative, and in online contexts are most easily engaged by hyperbolic framing (e.g., "clickbait" headlines, overstatement, simplification, and fallacious rhetorical style).[106] The process of circulating discourses through grievance works particularly well when points of affective attachment are found in less hyperbolic variations, often as common-sense beliefs, in normative social and political discourse.[107] In this way, affective attachments provide a bridge between offline and online space, such that users can relate to and reinforce the ideas they encounter online because of their offline experience and vice versa.[108] And affective circulation is a crucial modality of information flows in the context of gray zone information operations.

Spreadability, like publics theory, relies on analyses of circulation but focuses on how and why media artifacts move, as well as the implications and effects of which media circulate.[109] Moreover, spreadability foregrounds how digital and social media technologies enable multi-directional interactivity and position users as information sources, manipulators, and agents of spread. In this way, spreadability as a concept highlights how the new media ecosystem increases "participatory culture," which "now refers to a range of different groups deploying media production and distribution to serve their collective interests."[110] Spreadability as a framework for media circulation ingrains a socio-technical lens requiring attention to the interrelationship between users and technological features. Furthermore, the concept "suggests that the affordances of digital media provide a catalyst for reconceptualizing other aspects of culture, requiring a rethinking of social relations, the reimagining of cultural and political participation, the revision of economic expectations, and the reconfiguration of legal structures."[111]

Spreadability therefore sees the new media ecosystem not as a break from prior communicative and media technologies, but as a type of cultural system integrating technologies, people, and practices that develop and adapt in relation to each other. As such, there is no single reason people spread media. Rather, spreading media constitutes sets of choices that users and sources make for a variety of social, economic, and technological reasons. Thus, "we have to understand that the cultural practices that have both fueled the rise of these sharing technologies and evolved as people discover how these platforms might be used."[112]

The conceptual and analytical frames of publics and spreadability position circulation as an essential frame for understanding how the new media ecosystem interweaves people, technology, and communication through agentic, choice-based practices with cultural, economic, and sociopolitical effects. It is unsurprising then that the new media ecosystem is a primary site for gray zone information operations aimed at impacting global systems. Moreover, the prior success of information operations leveraging the new media ecosystem to impact each of these aspects—cultural, economic, social, and political—increases the likelihood that such multi-vector IO-driven strategies will continue to prove effective and efficient modes of hostile engagement.

4. Methodology: Applying Evolutionary Theory to Gray Zone Information Operations

It is from this context—the new media sphere, including convergence, participatory culture, and circulation—that this report turns to a relatively new methodology in security studies: evolutionary frameworks. This report applies evolutionary theory to understand the use of emergent technologies, specifically the techniques and procedures they enable, in the development of information operations as the means of gray zone competition. Yannick Veilleux-Lepage outlines how terrorist tactics, as "techniques of contention," evolve historically through processes of selection, adapt to their environment (e.g., state and political responses), and are transmitted between generations.[113] Veilleux-Lepage extends work by Charles Tilly on "repertoires of contention" by applying evolutionary theory to model the development of the use of airplane hijackings from the 1960s to the present.[114] The use of evolutionary theory, crucially, disentangles techniques from specific actors and events in order to better understand the larger context and scope of the generation, deployment, and development of practices that enable airplane hijackings (in Veilleux-Lepage's case).

In applying an evolutionary lens to IOs, this report seeks to get at the broader picture of information weaponization with an eye to dispelling common misperceptions and more accurately anticipating which IOs will predominate in the short, medium, and long-term. The units of analysis, an integral component of evolutionary models, for this study are propagation and mobilization techniques, which serve as the two primary lines of effort of gray zone IO-driven strategies. While propagation and mobilization are distinct ways to achieve a desired strategic end, in the new media ecosystem the techniques used to propagate media spread and mobilize action are often co-constitutive, such that IOs for propagation are necessary for mobilization and IOs for mobilization are productive of propagation. Gray zone IOs can be understood as having one of two impacts along these lines of effort, creating positive or negative feedback loops. Moreover, case examples make clear that some overall IOs have included creating both types of feedback to realize specified goals (e.g., the "both-sides" techniques of Internet Research Agency operations, wherein its operatives impersonated Americans on various sides of heated political disputes in order to sow chaos). Thus, specific propagation and mobilization IOs in the new media sphere can be understood to be utilized for one of two general purposes in controlling information flow: amplification and suppression. These two purposes—amplification and suppression—dictate which specific propagation and mobilization IOs will be selected and how they will be used. As such they can be viewed as repertoires, or "a limited set of routines that are learned, shared, and acted out through a relatively deliberate process of choice," as will be discussed in detail in the next section.[115]

4.1 Variation and Transmission

Using propagation and mobilization IOs as the unit of analysis for this report enables a discussion of the evolution of these IOs as socio-technical entities with a focus on their varieties (variation), adaptations by users and platforms, as well as their transmission to subsequent event "generations." As this report draws on Veilleux-Lepage's work regarding the application of evolutionary theory to the social sciences, it is worth quoting at length from his explanation of evolutionary theory in the biological context and how he specifically applies it to airplane hijackings.

First, in the biological context, Veilleux-Lepage explains the three major components of evolution: variation, transmission, and selection. He writes:

> The essence of the evolutionary argument is that most of the behavioural and physical characteristics of a species evolve because '[t]hose whose genes promote characteristics that are advantageous in

> the struggle to survive and reproduce are rewarded through the transmission of their genes to the next generation' (Kitcher 1985, 42). This process has three main components: (i) variation, that members of a relevant population vary with respect to at least one characteristic with selective significance; (ii) transmission (sometimes called heredity), that there exist copying mechanisms to ensure continuity over time in the form and behaviour of entities in the population; and (iii) selection, that the characteristics of some entities are better adapted to prevailing evolutionary pressures and, consequently, these entities increase in numerical significance relative to less well-adapted entities. In other words, the evolution of an entity within a system involves three key principles: variation, transmission, and selection.[116]

Veilleux-Lepage then goes on to explain his own methodology in applying these Darwinian principles to the airplane hijacking context:

> Each section applies a different Darwinian principle: (i) the variation sections identify the adaptations the technique underwent in the period and places in question and the factors that led to the emergence and mutation of these adaptations; (ii) the transmission sections concern themselves with identifying the mechanisms that led to the transportation of adaptations across different repertoires; (iii) the selection sections explore the contexts in which various techniques of variants of techniques are adopted or rejected by a multitude of claim-makers, looking at how techniques of contention are frequently assessed by those who use them (or indeed choose not to) on the basis of feasibility, legitimacy, and efficacy.[117]

We utilize a similar framework. In this report, we approach the complexities of the new media ecosystem in nuanced ways—for example, by looking at the information operations technique of algorithmic manipulation and how it varies across platforms and devices based on both the structures of the technologies (how they are built) and user-developed practices. This approach enables a view of how algorithmic manipulation, as a technique, has changed over time and through interactivity (e.g., across platforms, as a function of the development of influencer marketing, or in response to content moderation).

Variation, which we interchangeably refer to as *adaptation* in this report (as the two are inherently linked), is a process of evolution that can be assessed through exploration of propagation and mobilization techniques. Adaptation occurs on two primary levels: 1) technological development and 2) users' development of practice, aimed at maximizing the utility of the new media ecosystem to meet their goals. Adaptation by technological development is practiced by platforms and tech companies as they develop new algorithms, program features, apps, and new modes of digital and social mediation. These adaptations are generally driven by tech companies' attempts to maximize profit, increase user satisfaction, or avoid criticism or regulation. Recent adaptations have included *deplatforming* (banning users or content) and *algorithmic suppression* (when a company disallows recommendation or trending) of specific content, users, or accounts. This type of adaptation is a response to increasing demands for content moderation in relation to polluted information (e.g., extremist content, dis/misinformation, conspiracy theories) and the need to limit users' exploitation of their programs and features.

Adaptation of practice is performed by users who learn how to "game" affordances by using features in unique ways, who learn how to subvert or bypass rules to ensure content circulates, and who study how specific platform algorithms and personalization features work, then use that knowledge to increase their reach. One infamous case of user adaptation occurred in 2016, when Microsoft released its chatbot, an interactive, adaptive language-learning AI system known as "Tay." Tay was given the persona of a teenaged girl with the hope of engaging the 18- to 24-year-old population on social media for "playful fun."[118] Users, however, had other plans for Tay, and rapidly

"re-educated" her by "exploiting a repeat function" (she tweeted some 95,000 tweets in her first day), getting Tay to repeat racist, anti-feminist, and pro-Nazi, as well as offensive and abusive commentary. Oscar Schwartz recounted how trolls active on 4chan figured out how to provoke this behavior from Tay:

> In a coordinated effort, the trolls exploited a "repeat after me" function that had been built into Tay, whereby the bot repeated anything that was said to it on demand. But more than this, Tay's in-built capacity to learn meant that she internalized some of the language she was taught by the trolls, and repeated it unprompted. For example, one user innocently asked Tay whether Ricky Gervais was an atheist, to which she responded: "Ricky Gervais learned totalitarianism from Adolf Hitler, the inventor of atheism."[119]

Microsoft attempted to correct the issue, taking Tay offline, cleaning up the program, and re-releasing a new chatbot, Zo, which was programmed to shut down offensive or sensitive discussions, including politics and religion. Unlike Tay, if Zo were repeatedly pressured "to talk about a certain sensitive topic, she left the conversation altogether, with a sentence like: 'im better than u bye.'"[120] Tay is but one example of how users' creative approaches to technological features can exploit them in ways developers and companies had not considered. In addition, services (businesses) have developed to enable users' manipulation of platform algorithms and rules. For example, users can purchase engagement (e.g., followers, likes) to rapidly build their brands.[121] Most recently, businesses have been identified that will utilize bots—automated computer programs—to enable users to attack other users by submitting mass numbers of erroneous rules violations reports with the intent of getting the target user suspended or banned from the platform.[122]

Along with technological development and related user practices, common internet cultural norms for adaptation of digital media work as IOs of propagation and mobilization. The most recognizable framework for adaptation in this sense is meme culture. *Memes*, a term coined by Richard Dawkins in the late 1970s, refers to the way bits of culture seem to replicate and move through society.[123] A meme can arise out of any cultural milieu, but today most often reference "internet memes—the linguistic, image, audio, and video texts created, circulated, and transformed by countless cultural participants across vast networks and collectives," shared widely on digital and social media.[124] Memes are exemplars of the participatory cultural practices generated in the new media ecosystem, which blurs the lines between producers and consumers through the reappropriation and reuse of texts to circulate discourses, often using emotive frameworks such as humor and irony as a mechanism of spread.[125] Ryan Milner argues that "memetic media are aggregate texts, collectively created, circulated, and transformed by countless cultural participants. They're innumerable—as dense as they are vibrant—and understanding their implications for public conversation requires understanding intertextual connections, even when assessing singular texts."[126] Thus, memes work as cultural adaptations of digital media that enable propagation and mobilization information operations rooted in discourse and utilizing the new media ecosystem. Crucial to the weaponization of information through meme cultures are specific social networking sites like 4Chan, 8Chan, and EndChan, which are sources for much of the development of meme cultural adaptations, including topical and discursive framing, aesthetics, and modes of circulation. For example, the cooptation of the now-infamous Pepe the Frog memes and cooptation of the "OK" hand gesture utilized by alt-right and far-right cultures online began as networked campaigns on the Chan boards spurred by users' sense of "edginess" and a desire to "troll the normies" (internet slang for normal people who don't understand or subscribe to in-group cultures of the internet, such as Chan culture).[127] The advent of networked campaigns to co-opt symbols like Pepe the Frog, the OK hand gesture, and other cultural touch points foreground a discussion of transmission of IOs that drive propagation and mobilization .

Transmission of propagation and mobilization strategies occurs through multiple processes in the new media ecosystem. In some cases, transmission of strategies is direct, with users telling others how to promote their content more effectively. Direct transmission also encapsulates the rise of paid forms of training, such as workshops, college courses, and other formal learning methods. In many cases, platforms themselves offer blogs and "training" media targeted at users, primarily those seeking to become influencers, with platform-specific strategies for success, news of new feature and program rollouts, and success stories aimed at encouraging users. Transmission also occurs through less direct means, including users' copying of other users (*wow that was cool, I am going to try it*). Indeed, user practices are seen and thus transmitted to other users as a function of networked engagement. Within this frame, virality (discussed in more detail in the next section) becomes essential to understanding how strategies of propagation and mobilization are viewed as successful and then reused. Another increasing method of transmission is gamification, or the use of gaming components and practices, such as rewards, leaderboards, etc. in non-gaming contexts.[128] Gamification works to motivate participants to produce particular social behaviors and actions. In the violent extremist context, the livestreaming of the Christchurch Mosque attack encouraged followers to share and spread the video, which was quickly banned. However, users employed additional methods of gamification to keep the Christchurch attack content circulating and thus subverting the bans on it. This included propagation strategies such as memeification (converting parts of the livestream into memes) or sharing video and stills from the livestream along with other mass attacks with added leaderboard style "kill counts" as methods of "gaming the system."[129]

4.2 Selection Factors: Feasibility, Legitimacy, Effectiveness

This report's evolutionary framework highlights analyses of variation and selection to understand the rapidly changing technologies and practices of information operations in the new media ecosystem. It requires attending to selection factors such as feasibility, legitimacy, and effectiveness, which indicate which propagation and mobilization strategies will continue to be used, adapted, and transmitted, and which will likely die off. Selection factors in digital and social media contexts are also governed by the interaction of people and technology and are thus dependent, in terms of scalar uptake, on the combined effects of access (cost), skill (users' capability), and ease of use (technological functionality). The shift from Web 1.0 to Web 2.0 technologies provides an instructive example, as declining costs of equipment and access connected with increasingly easy-to-use system interfaces, thus enabling a huge influx of users with limited computer skills (e.g., coding, programming) to become content producers in the digital space with little to no training.

Feasibility, as a framework for selecting IOs to enable propagation and mobilization, thus considers both producer and consumer standpoints (tech that makes creating, sharing, and participating) both easier and more lucrative in financial, social, or operational terms. Feasibility must also consider technological and platform factors such as content moderation. Going back to the Christchurch attack example, bans led to the generation of multiple techniques to continue to propagate the livestream video, such as users who rebuilt the entire 45-minute attack livestream in virtual environments like Roblox (a game environment). Rebuilding such a long event is a time and skill intensive endeavor, requiring compelling motivation on top of other factors. Thus, analyses of feasibility as a selection factor can expose the weighting of social or technological aspects of user choices.

Legitimacy is also an IO selection factor for propagation and mobilization in the context of media spread and gray zone information operations. The new media ecosystem tends toward heuristic frames for determining information legitimacy. Heuristics are cognitive short hands that people use to increase the efficiency of processing new information and situations.[130] The Elaboration Likelihood Model (ELM) of information processing, a framework for analyzing persuasive communication, shows that as heuristic thinking increases, elaboration (critical thinking)

declines.[131] Importantly, common heuristics such as credibility (is a platform, source, or message credible), consensus (do others agree/disagree with this message), and likeability (is the source trustworthy) are often utilized in digital and social media contexts, given the vast quantities of information users parse and consider.[132] Importantly, heuristic thinking is promoted by both human information processing and features built into social media platforms. For instance, consensus heuristics may be engaged by now-common emotion/emoticon response features (e.g., likes, favorites, dislikes) potentially increasing a reliance on heuristic thinking in the selection of which information to engage and share. Trends such as influencer culture also increase reliance on heuristic thinking, specifically by engaging the likeability heuristic through an influencer's ability to project authenticity and trustworthiness as a framework for building credibility among their followers. And as more people rely on digital and social media for news consumption, credibility heuristics are engaged by platforms, brands, and pundits, particularly through consistency heuristics. Similar to the concept of confirmation bias, people rely on consistency as a heuristic principle in determining if new information is credible based on its correspondence (consistency) with their existing beliefs. An example of this is the use and spread of the moniker *fake news* as a shorthand (heuristic) category for platforms, sources, and messages identified with partisan political positions, regardless of the actual information being shared.

Decreases in elaboration in relation to digital and social media have been discussed widely. For example, they have been discussed with respect to users sharing posts, including stories and news articles, based on their headlines or other posters' commentary without ever clicking the story to actually read the material.[133] This has become so regular that major social media platforms like Twitter have created features that flag users as they share items with a notice if they have not opened the article they are sharing. Similarly, Facebook has increased its use of public informational flags on certain materials, such as COVID-19 mis/disinformation.[134] Many legitimacy flagging features were released by various platforms in response to calls for increased content moderation due to prominent uses of mis/disinformation (e.g., related to election messaging or the novel coronavirus). While it remains to be seen if these relatively recent features will have a broad effect, they clearly respond to the increasingly widescale spread of polluted information. Users have also developed their own frameworks for judging information, particularly source legitimacy. For example, on Twitter users frequently look at account stats and individual tweet stats to determine legitimacy. Recent account creation dates combined with low numbers of followers is a framework users discuss for identifying bot activity. For individual tweets, their "ratios"—when the number of replies to a tweet vastly outnumber the likes or retweets of the original post—are said to indicate the low value (illegitimacy) of the message.[135] "Ratios" are thus used to determine illegitimacy, rather than analyzing message veracity. They act essentially as a negative popularity contest over the message and promote alternate positions by negatively amplifying the delegitimated message through like-minded user mobilization. Here, success in delegitimating a tweet is determined by the size of the user population mobilized against it. Each of these practices relies on Twitter's visible platform statistics (account, follower, like, and retweet data) to generate platform-based credibility and consensus heuristics for users. Both platform-developed (technological) features and user-developed legitimacy practices highlight the issue of effectiveness as necessary to the selection of propagation and mobilization techniques.

Effectiveness as an IO selection criterion of specific propagation and mobilization lines of effort is dependent on other factors related to the strategic end state of a gray zone actor. These include which IOs are adapted for feasible use in circulating information in preferred digital contexts (e.g., singular platforms, cross-platform proliferation, spread to mainstream media), which user groups are targeted (e.g., niche groups, partisan groups, general groups), as well as which strategy repertoires would provide the best outcomes (e.g., amplification, suppression, or both). Benchmarks for effectiveness may also vary, ranging from basic reach and positive response (likes and shares), to changing socio-political discourse (amplification/suppression of topics), to inciting polarization (using both amplification and suppression to harden divisions), to mobilizing on-the-ground action (increasing protests or

decreasing voting). The most effective IO strategies will likely be used again for similar types of strategies until they become less effective or newer, more effective options become available.

Importantly, not all effects or outcomes of information operations can be determined in advance. There is always a degree of unpredictability in ways that people and technology will respond. For example, one of the most highly effective recent information operations, QAnon's hijacking of the Save the Children campaign hashtag, spread and mobilized action well beyond any earlier QAnon operations. In this case several factors—such as increased audiences due to pandemic lockdowns, along with people's fears and anxieties because of rapidly changing information about the pandemic—helped create a perfect storm for information spread. Moreover, the information operation, rather than being centrally planned, was carried out through a loose network of influencers from a variety of positions (e.g., conspiracy theorists, far-right extremists, anti-vaccine proponents), likely with different frameworks for technique selection and ideas of effectiveness. Importantly, the outcome was a rapid, large-scale spread of the campaign through online parenting, specifically mothering, communities, which comprise a vast, global network of users connected across digital and social media.[136] While the campaign spread across multiple platforms, it became near ubiquitous for several months on Instagram and its parent company Facebook. This spread was dubbed "Pastel QAnon" because of its use of pastel hued memes (many made on the media production service Canva) that worked to soften and normalize the conspiratorial messaging.[137] This campaign radicalized many new participants, increasing their broader engagement with QAnon conspiracy theories and subsequently with other related messaging from far-right extremists. The campaign also successfully mobilized a sustained wave of street mobilizations (protests) in the United States, U.K., and Europe throughout the late summer and early fall of 2020.[138] This campaign marks the effectiveness of hashtag hijacking (cooptation) as a mode of not only spreading but normalizing extreme ideologies and conspiracy theories.[139] This IO-driven strategy could continue to be adapted and deployed by groups seeking to radicalize or otherwise influence broad sectors of the population.

Determining the effectiveness of propagation and mobilization lines of effort used by various actors is generally based on comparing the desired effects and outcomes of the strategy with the actual effects and outcomes. This has led to a focus on specific actors rather than on the IOs used within the new media ecosystem, thus limiting the perspective of how they shape and support the developments of gray zone strategies. The remainder of this report details IOs that result in specific propagation and mobilization outcomes to provide a more comprehensive view of current and potential threats. By incorporating examples of both general and gray zone usage of information operation, this report highlights how their interrelationship affects their evolutionary trajectory.

5. Propagation of Perspective

Information operations are rooted in actors' development of their ability to shape the perspectives of publics using communication technologies. Shaping the perspectives of groups of people in the new media ecosystem requires technical and cultural facility with a variety of platforms and technologies. And, perhaps most importantly, shaping perspectives requires human cultural awareness across a variety of dimensions, including the identity-based and political intricacies of selected target populations. Thus, the propagation of perspective is a socio-technical process that weaponizes information and cultural relations to achieve strategic goals. The following section outlines the socio-technical processes that enable the propagation of perspective within the new media ecosystem by leveraging its characteristics—interactivity, convergence, and access to vast quantities of data—to circulate information.

Propagation of perspective relies on altering the ways in which information circulates among and between publics. Propagation, in this sense, includes both spreading and limiting the spread of information. This may mean capitalizing on existing informational spread (e.g., co-opting an existing campaign or topic), creating specific content

or information framing to spread (e.g., troll/bot farms that generate content), or exploiting contested information environments (e.g., using a public debate to inject conspiracy theories). Along with this variety of information shaping frames, the interactivity of the new media ecosystem allows for propagation through interactions between various media sources (mainstream, alternative, influencer, platform, and user). For example, extremist content from the alternative media has been propagated by mainstream media in news stories, as well as by influencers and users who share either original content or news stories about extremist content.[140] Such interactive propagation is easier to achieve through convergence culture and enabled by the massive scope of available news and data online.

5.1 Information Circulation Repertoires

Information can be either amplified or suppressed by IOs. The specific IOs to shape perspectives through amplification and suppression are similar, technologically speaking. It is, however, the way they are used and their combinations of usage which affect the intended (and perhaps unintended) ends. Thus, the IOs can be viewed as sets, or repertoires, through which amplification or suppression are achieved. Key IOs discussed in the following sections include affordance and algorithmic manipulation, networked harassment, and multi-platform efforts, as well as trolling, virality, deplatforming, and political astroturfing (making an IO look like a grassroots movement). These techniques can largely be put to use for either amplification or suppression. The one exception is the technique of deplatforming, which has a primarily suppressive direct function, although actors have been able to leverage it into an indirect amplifying function through ongoing debates over digital free speech. Importantly, the combinations of IOs can be targeted for localized or large-scale (scalar) impacts, depending on the groups, publics, or populations targeted for perspective shaping.

Viewing sets of IOs used to amplify or suppress information draws on Charles Tilly's notion of "repertoires of contention," which describes how sets of claim-making performances (e.g., petitioning, demonstrating) "clump into *repertoires* of claim-making routines" that are both limited by their situational norms and improvisational in their application.[141] This frame allows for complex analyses of information operations that can delineate both the IOs used in the operation as well as IOs used in response, to better understand the selection factors of the immediate operation as well as the operation's variations and adaptations from other IOs. For example, analyzing an IO that uses bots, political astroturfing, and trolling could include: 1) delineating how each technique is used (its function—amplifying, suppressive, or both—within the IO), 2) how the three techniques work together to affect specific outcomes, and 3) how these uses (individual and combined) vary from or adapt uses of the techniques in other IOs.

Because most of the IOs examined in this section can be deployed to both amplifying and suppressive ends, we discuss each repertoire from the position of purpose and provide an exemplar case—the ongoing COVID-19 origin debate—to show how the repertoires work and interact within the new media ecosystem.

5.2 Amplification Repertoires

Amplification increases the spread and intensity of messaging. It can be achieved through human creative means or by technological (often algorithmic) means. Examples of creative amplification include marketing approaches such as writing clickbait headlines, using sensational or controversial story framing (e.g., "if it bleeds, it leads"), and memeifying socio-cultural events or topics (e.g., the "Karen" meme).[142] Examples of technology-driven, often platform-based, approaches include algorithmic features on digital and social media, such as trending topics, top stories, and notifications systems that guide users to increased engagement with and spread of content. Furthermore, these two forms of amplification—human creativity and technological—are often interactive and overlapping in the new media ecosystem. For example, sources (e.g., influencers, users) who learn how to manipulate platform

algorithms (e.g., attaching trending hashtags, images, or songs to their content) and engagement indicators (e.g., buying likes, followers, or even up/down voting content) can consequently circulate their content more widely.

In information operations, amplification is produced through the interactivity of human and technological amplification methods. This can take crowd-sourced or paid forms. Crowd-sourced coordinated campaigns (e.g., GamerGate, the Fappening, SavetheChildren, StoptheSteal) rely on interested individuals connected by dense online networks who coordinate their actions to amplify their message and shape perceptions. In these amplification efforts, "troll armies" of users participate in the attacks and propagation of information as a social activity and perhaps also for entertainment.[143] In some cases, the focus of the amplification is networked harassment (e.g., incessant violent messaging, threats, and doxxing aimed at specified "enemies") which grows over time as other like-minded users within and across these networks see what is happening and join in.[144] In some cases, bots and fake accounts being run for other information operations may find it useful to join these crowd-sourced amplification efforts—particularly politically-focused efforts—to advance their own goals. Primarily these types of amplification are meant to be seen and are designed to make targets and wider user populations "know" what is happening. As such, these efforts are not covert or conducted in a non-attributable way. Rather, they tend to publicly discuss and organize their efforts in fora and on public platforms to engage more support, amplify and maintain the momentum of the message.

Sophisticated coordinated amplification lines of effort may be run by marketing firms or in-house specialists (as with the Internet Research Agency) to promote specific entities (e.g., individuals, companies) or forward state interests. As these paid amplifications efforts are meant to be covert, they are inherently difficult to trace, thus preferring human-controlled fake accounts for content propagation and limiting bots and automated features to contexts where exposure will not undercut the campaign (e.g., to spam other accounts or to discredit other individuals). Such efforts also often target influencers, to engage them as amplifiers in their own networks.[145] These uses of bots, fake accounts, and automated trolling have been identified by Howard and Wolley as integral components of "computational propaganda," or the "assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion," including automated political influence, disinformation, and so-called fake news.[146]

Amplifying a perspective or message inherently suppresses other possible perspectives or messages to some extent. For example, trolling as an amplification tool to engage a specific audience may also have a suppressive effect on the targets being trolled, who may seek to limit further conflict. Similarly, agenda-setting tactics used to amplify a message (e.g., "trading up the chain," or planting bait stories in the hope that mainstream media will pick up and amplify the stories) work to shift perspective through strategic (re)framing of stories and events, thereby suppressing other possible perspectives.[147] That sort of passive suppression, however, is a second-order consequence of amplification repertoires rather than a function of specific suppression repertoires.

5.3 Suppression Repertoires

Suppression as an IO tool is a set of practices that work to the opposite purpose of amplification. Counterintuitively, suppressive tools can be coordinated with amplification rather than conflicting with it. And suppressive techniques are also used by platforms, media sources, and users in response to adversary information operations, or in attempts to reshape perspectives in ongoing debates. As with amplification repertoires, suppressive ones blend human creative action and technological capacities. Unlike amplification tools, suppression has more explicitly bifurcated creative and technological approaches.

Human creative approaches to suppression are often dependent on negative social reactions and even moral outrage as a triggering mechanism. These tools include public shaming by so-called "online mobs," calls to demonetize transgressors (e.g., firing, pulling of sponsors), and choices by media companies, news aggregators, or influencers to ignore stories or openly stigmatize certain ideas. Suppression can also flow from the mainstream media to digital and social media. The mainstream media performs a strong information agenda-setting function by selecting which stories to cover and how those stories are framed. This holds true regardless of any particular media outlet's political perspective (liberal, moderate, conservative).

Importantly, these suppressive mechanisms work through direct suppression of specific sources, content, ideas, or stories, but may also contribute to the development of broader silencing effects through a social phenomenon known as a "spiral of silence," where users may self-censor based on their perception that sharing/posting things other users don't agree with might cause them harm. For example, on July 7, 2020, an open letter titled "A Letter on Justice and Open Debate," was published by *Harper's Magazine* online. The letter stated:

> The free exchange of information and ideas, the lifeblood of a liberal society, is daily becoming more constricted. While we have come to expect this on the radical right, censoriousness is also spreading more widely in our culture: an intolerance of opposing views, a vogue for public shaming and ostracism, and the tendency to dissolve complex policy issues in a blinding moral certainty. We uphold the value of robust and even caustic counter-speech from all quarters. But it is now all too common to hear calls for swift and severe retribution in response to perceived transgressions of speech and thought. More troubling still, institutional leaders, in a spirit of panicked damage control, are delivering hasty and disproportionate punishments instead of considered reforms.[148]

Signed by more than 150 artists, academics, and writers, the letter's critique of social suppression notes: "The way to defeat bad ideas is by exposure, argument, and persuasion, not by trying to silence or wish them away.... As writers we need a culture that leaves us room for experimentation, risk taking, and even mistakes. We need to preserve the possibility of good-faith disagreement without dire professional consequences."[149] Essentially, spirals of silence suppress ideas by creating a sense that espousing unpopular or stigmatized ideas may incur unreasonable personal or professional costs.

Technological approaches tend to be the primary province of platforms (companies) rather than users. These approaches include algorithmic suppression, banning, and deplatforming (removal from platform or platform denial). Importantly, these two frames, while bifurcated, also may work in coordinated ways as rising human creative responses may lead platforms to respond by implementing technological suppressive measures, or lead companies to respond by disassociating with or firing transgressors. For example, Facebook "demonetized" *Epoch Times* accounts on its platform by technologically disabling their ability to advertise. Facebook maintains that this action was policy enforcement of the *Epoch Times*'s attempts to evade verification rules surrounding political advertisements that were designed to prevent potential foreign influence of elections. The *Epoch Times* maintains that its advertisements are not political ads, but instead are outreach to increase subscriptions. The *Epoch Times* retains a non-advertising presence on Facebook but has moved its advertising to another platform, YouTube, where the publication is not required to disclose spending on political ads.

Alternatively, technological approaches used by non-platform actors generally fall into methods used to manipulate platform affordances (features and capabilities) and are used to support amplification strategies. For instance, a coordinated network of fake accounts or bots on a forum site like Reddit can work to downvote posts to suppress certain content, ideas, or stories.[150] In this way, the networked users can manipulate trending topics and top posts, influencing which posts are seen and engaged with.

Suppression of information as a way for shaping perspectives, while common, can be difficult to deploy covertly in the new media ecosystem. The characteristics of the new media ecosystem enable identification and contestation of suppressive (or perceived suppressive) tools, particularly agenda-setting methods used by the mainstream media, as well as the promulgation of a variety of alternate information (stories, ideas, content, sources) and interpretations. Such difficulty is exacerbated in relation to politicized topics in the current cultural context of political polarization and distrust in institutions (specifically the media).[151] This is clear in ongoing free speech debates in relation to digital and social media, which assert that platforms have an anti-conservative bias, and regularly suppress, ban, and deplatform conservative content and sources. It is a claim that has mobilized the development of multiple conservative "free speech"-focused social media platforms, such as Gab, Parler, and Gettr. Simultaneously, liberal and progressive sources and users also claim that platforms are biased, but in favor of conservative sources and content. Additional platform behaviors, particularly lacking transparency regarding content moderation practices and algorithmic changes, likely increase widespread perceptions and claims of suppression. Furthermore, irregular application of platform rules concerning content and user behavior similarly increase contention about platform censorship.

The politicization of debates about suppression problematically offers vectors of information exploitation. Because a major point of contestation over the suppression of information is who gets to determine which information is acceptable and which is not, institutional media's agenda-setting provokes partisan distrust that can be exploited in digital and social media debates. Furthermore, the politicization of concerns over technological suppression works to obscure necessary discussions about digital and social media platforms' role, responsibility for transparency, and scope of responsibility for content on their platforms (e.g., overhaul of Rule 230 of the U.S.'s Communications Act) and how potential regulation might be achieved in a manner that protects speech rights.

To better explicate the intricacies of how amplification and suppression repertoires work in the new media ecosystem, an extended example exploring media (traditional, digital/social, mainstream, alternative, platform, and user) coverage of and responses to the ambiguities concerning the origins of COVID-19 is illustrative.

5.4 Propagation of Perspective in Action: COVID Origins

The origins of the novel coronavirus COVID-19 have been a point of speculation and debate since the World Health Organization publicly announced a new "pneumonia-like" illness in Wuhan, China, on December 31, 2019. Just a few days later, on January 5, 2020, the first social media post positioning the still-unnamed virus as created by the Chinese government emerged from a user in Hong Kong who claimed it was being intentionally spread around the globe.[152] Meanwhile, news reports about the illnesses in Wuhan drew a connection to a local live animal (wet) market, suggesting a natural transmission via a jump from animal to human populations.[153]

The intentional release narrative that was first raised in Hong Kong also drew upon conspiracy theories holding that the 2003 SARS epidemic was manufactured by China and intentionally released to harm the people of Hong Kong. The tweet arguing that COVID was manufactured in China stated that "18 years ago, #China killed nearly 300 #HongKongers by unreporting #SARS cases, letting Chinese tourists travel around the world, to Asia specifically to spread the virus with bad intention. Today the evil regime strikes again with a new virus."[154] At the time, the natural transmission narrative of animal-to-human migration of the virus in a live market seemed to align more closely with received wisdom and accepted scientific knowledge.

Some early discussions of COVID's origins introduced the fact that a Wuhan virology lab had been working on coronavirus research, thus suggesting the possibility of a lab leak. However, the mainstream media endorsed the natural transmission narrative, treating the lab leak hypothesis as a conspiracy theory.[155] This was furthered by some

scientists labelling it as such. The medial journal *Lancet*, for example, published a statement from 27 scientists that condemned what they described as "conspiracy theories" about human involvement in the creation of COVID. It was later learned that "one of the organizers of the statement was ... the head of an American organization" that funded a virology institute in Wuhan that conducted experiments with the coronavirus, and thus seemingly possessed an undisclosed conflict of interest.[156] NPR's coverage of the lab leak hypothesis at the time was typical of mainstream media treatment of the issue. NPR reported that there was "virtually no chance" that COVID-19 had originated in a laboratory in China, as an accidental release "would have required a remarkable series of coincidences and deviations from well-established experimental protocols."[157]

In the United States, information about the virus, its origins, and protocols for action were constantly shifting due to both the incorporation of new data and a lack of a fully coherent approach within the federal government. Different agency approaches aligned with their respective concerns and missions—e.g., public health, economics, national security—which confused messaging to the U.S. population. For example, public health concerns about shortages of personal protective equipment (PPE) initially governed messaging that masks were not indicated for use by the general public. When public health officials later declared masks necessary for general use, confusion and distrust of government messaging increased.[158] Moreover, messages about preparing for the pandemic were broadcast and then walked back by some officials—not least by President Trump, who insisted early on that the virus wasn't a big problem and would quickly disappear.[159]

Additional complicating factors included mis- and disinformation spread by China accusing the United States of creating the virus as part of a military operation intended to demonize China, as well as Russian and Iranian mis- and disinformation about the virus. In response to PRC-backed claims, and in light of China's position disallowing researchers from other countries to study the origins of the virus in Wuhan, there was early speculation in some quarters that the virus had leaked from the Wuhan virology lab. Additionally, President Trump regularly referred to COVID-19 as "the China virus" and "the Kung Flu" in his rallies and speeches, drawing on language used on social media by members of his base.[160] Further, hostility toward and violent attacks against Asian Americans increased, with advocates and activists linking these attacks "to rhetoric that blames Asian people for the spread of Covid-19."[161]

In this context, mainstream center-left and left-leaning news outlets initially generally suppressed the lab leak hypothesis, instead amplifying "mainstream" scientific claims that the virus was of natural origin. On the other hand, center-right and conservative-leaning news outlets ran stories raising the lab leak theory. Conservative politicians—including Senator Tom Cotton, President Trump, and Secretary of State Mike Pompeo—promoted claims that China could be covering up a lab leak (or, worse, covering up the intentional development and release of COVID-19).[162]

Throughout 2020, the debate over the origins of COVID-19 continued. The mainstream media generally continued to avoid discussion of the lab leak hypothesis even as more drips of information potentially supporting a review of the lab leak theory emerged. This included information on NIH-funded "gain of function" research: a controversial type of virological research being conducted in Wuhan in which experiments aimed to increase the infectiousness of viruses in order to better understand how to combat them. Further information concerned the genetic similarity between COVID-19 and a strand found in China in 2012 that was collected for research at the same lab.[163] Such new information led to increasing calls to revisit the possibility of an accidental lab escape as the virus's origin. The later reporting on the lab leak hypothesis was revelatory of how successful suppression efforts had been in the mainstream media sphere. For example, former *New York Times* science reporter Donald G. McNeil Jr. had written a 4,000-word story about the lab leak hypothesis, which he had titled "New Coronavirus Is 'Clearly Not a Lab

Leak,' Scientists Say," that the *Times* ultimately chose not to publish. The *Washington Post* details how, once widely described as a conspiracy theory, the lab leak hypothesis burst into the mainstream in 2021:

> The journalistic reconsideration of the lab story has been told not just in probing new stories — The Washington Post has published five stories about it on its front page in the past 2 $^{1}/_{2}$ weeks, some prompted by President Biden's order of a 90-day review of the theory by intelligence agencies — but in corrected headlines and in editors' notes affixed to last year's stories. New information often casts out old, but it is unusual for news outlets to acknowledge so publicly that they have changed their understanding of events.
>
> The retroactive takes seem to raise a theoretical question: Were news reports diminishing or disregarding the lab-leak theory actually "wrong" at the time, or did they in fact accurately reflect the limited knowledge and expert opinion about it?
>
> To some pundits, the early dismissals of the lab thesis now look like media malpractice. "The media's credibility is taking yet another hit," Dan Kennedy, a veteran media critic and college professor, wrote earlier this month. He suggested the alleged mishandling of the story last year "may make it that much harder to persuade Trump supporters to get over their skepticism about vaccinations."
>
> But that analysis has the great advantage of hindsight. Many scientific experts were dismissive of the leak theory at first, thus validating the early skeptical reporting. As with any story that is new, complex and evolving, conventional wisdom undergoes a metamorphosis as new information arrives.[164]

This description of later events—including the correction of earlier headlines and an affixing of notes to stories that had run the previous year—is indicative of a dramatic reversal. We do not intend to answer whether mainstream media suppression of the lab leak hypothesis was right or wrong; as the *Washington Post* notes, it is a complicated question. Instead, our point is that there was both mainstream media suppression of this COVID origin story and intensely polarized media positions surrounding it. This dynamic created space for mis- and disinformation, including conspiracy theories.

For example, one conspiratorial thread related to the lab leak hypothesis rests on stories that one of the virology labs in Wuhan, the Wuhan National Biosafety Lab, had previously conducted bioweapons research. This information, which was reported by the *Washington Times*, was then construed by some as evidence that COVID-19 was a Chinese bioweapon intentionally released to cause the pandemic.[165] Further conspiracy theories argued that, as a bioweapon, COVID-19 was designed to target specific ethnic populations. The reach of this conspiracy theory was global. As a DFR Lab report on the weaponization of COVID-19 rumors notes:

> The narrative that China created COVID-19 as a bioweapon reached a new level of narrative spread after *Great Game India*, an obscure Indian geopolitics blog with a history of publishing conspiracy theories, published an article claiming that Chinese spies had stolen coronavirus samples from a Canadian lab and weaponized it. Even though this article did not receive significant engagement initially, it was republished and amplified by fringe US websites such as *ZeroHedge*, known for spreading falsehoods and conspiracy theories.[166]

As this example illustrates, the confusion and partisanship of the informational messaging and news media coverage about the origins of the virus created vulnerable sites for information exploitation by state and non-state actors.

Inconsistent institutional messaging, mis- and disinformation, and partisan news coverage of the pandemic and its origins—dubbed an "infodemic" by the World Health Organization—had a material impact on the trajectory of the pandemic and its effects, including the politicization of non-drug-related tactics for slowing the virus (e.g., mask wearing, lockdowns, school closures, and social distancing).[167] These dynamics also had an impact on infection rates and deaths due to increased concerns about vaccination tied to mis- and disinformation. A notable case was the rapid spread of the film *Plandemic*, which propagated conspiracy theories about world governments, institutions, and global elites attempting to control people through the deployment of manufactured viruses.[168] Further, the film's creators mobilized online propagation of their content by asking viewers to share and repost the film as it was banned by platforms, and leveraging users' subsequent bans for sharing the film to promote the notion that the film's truths were being suppressed. The film was seen and shared by millions of digital and social media users worldwide within days of its release.[169]

Public anxiety concerning the virus, frustration at the lockdowns and their economic impact, and social isolation created a highly exploitable information propagation and mobilization environment for gray zone and other information operations. In concert with the mis- and disinformation circulating in the new media sphere, the COVID-19 pandemic provided an ample base for individual and large-scale mobilization, including anti-mask and anti-lockdown protests and increased radicalization to extremist ideologies.

6. Information Operations Methods in the New Media Sphere

Gray zone information operations in the new media sphere require facility and creativity in the use of digital and social media alongside existing practices of information operations in traditional broadcast and print media. As such, the information operations tools used in contemporary information environment are adaptive and may change in line with the development of new technologies, platforms, interfaces, and platform policies and user preferences. For example, as mainstream social media platforms such as Facebook or Twitter apply content moderation and user behavior policies, some users have migrated to alternate platforms such as Gab or Telegram. New platforms regularly emerge, and existing platforms regularly seek to keep users engaged through new feature development. There are crosscutting informational modalities shaped by online/digital cultural practices and norms that impact how information can be amplified, suppressed, or tainted in strategic ways. These crosscutting modalities rely on the characteristics of the new media sphere, particularly interactivity and access to high volumes of data, as well as online cultural norms such as participatory mediation (e.g., memeification, gamification, sampling).

The ability to manipulate information communication technologies is a crucial information operation tool. Such manipulation can be achieved in localized operations or at scale. Localized efforts include affordance manipulation and evasive tactics. Scalar methods include use of multiple platforms and algorithmic manipulation. These various efforts can range across platform-specific, cross-platform, and multi-platform uses that may change up or down in scale depending on operational considerations or technological developments. For example, hashtags were originally predominant on Twitter but not ubiquitous on other platforms, so hashtag hijacking had a limited, single-platform scale and effect. However, as Twitter has come into wider use, and as additional platforms have been developed with hashtag use embedded along with smart technologies enabling easy sharing of posts between platforms, users' preference for hashtag use has become ubiquitous across many social media platforms. This user preference combined with technological development has shifted the utility of hashtag hijacking (using an existing popular hashtag to circulate unrelated content) from a localized, platform-specific method to a large-scale tool that can impact multiple sites simultaneously and expose exponentially more users to messaging.

Affordances, in the new media sphere context, are sets of features specific to particular software or platforms. Users often utilize these features in ways that developers have not planned in order to achieve their own goals. Users often manipulate affordances to amplify or suppress messaging. For example, on platforms that rely on hashtags to circulate posts, hashtag hijacking has become a common framework that users employ to amplify messaging (e.g., QAnon's use of SavetheChildren, or ISIS's use of World Cup, Ferguson, and disaster hashtags). But this affordance does not work on platforms such as Telegram, which does not use hashtags to circulate posts, but rather uses them as an internal labeling system for group administrators.

Evasive IO methods, like affordance manipulation, are localized methods employed to evade content moderation and suppressive measures (e.g., detection, content removal, suspension/banning, deplatforming, demonetization). These may include anonymizing methods, such as the use of sock puppet (fake) accounts, the use of virtual private networks (VPNs), or the onion router (TOR) network to surf the web. Each of these capabilities work by masking the identity and digital information of users. Additional forms of "alt-tech" platforms (e.g., Gab, Parler, Mastadon) and distributed, peer-to-peer networks that are decentralized and rely on blockchain technology (e.g., Odysee, Dlive, Pando, BitTorrent) are also used to evade content moderation and removal.

Information Circulation Characteristics

"New" Media Sphere
- *Interactive*
- *Multi-Directional Information Flows*
- *Monetized and Non-Monetized*
- *Casual and Professional Producers*

Traditional Media:
- *Passive*
- *Uni-Directional Information Flows*
- *Monetized*
- *Professional Producers*

Often marketed as sites committed to digital freedom (e.g., freedom from moderation or surveillance), alt-tech platforms make it easier for users to work around laws, regulations, of other platforms' terms of service, potentially providing hubs useful for replacing banned content or providing back-up channels for accounts that might be banned. As such, alt-tech platforms don't simply provide ways to evade regulation and oversight, but also provide new sites for the amplification of information, particularly content that is likely to be suppressed on other sites. As the use of alt-tech, distributed peer-to-peer networks, and blockchain technologies develop and become more common, it is likely that new methods will emerge related to the specific affordances of these technologies.

Algorithmic manipulation also occurs on single platforms (as each has its own algorithms), but it can have an impact on a larger scale than affordance manipulation. Along with algorithmic manipulation, multi-platform IOs provide additional scalar options for information operations. Multi-platform IOs utilize coordinated, multi-pronged capabilities rooted in cross-posting messages and outlinking (posting links to content on external sites) to additional content on a variety of social media sites. This type of multi-pronged coordination is most commonly found in influencer and 360 degree marketing. The goal is to flood the information environment with the preferred messaging to build "buzz" around a topic or mobilize audiences. Multi-platform capabilities are coordinated through affordance manipulations like hashtag hijacking but work at scale due to the volume of platforms (messaging channels) being used. They can also include "astroturfing"—deceptive, organized online marketing

designed to look like organic grassroots responses and commentary—as a mechanism for amplifying messaging. Thus, multi-platform capabilities use influencer models, large-scale hashtag hijacks, and astroturfing as vectors of access in the digital/social media sphere in order to propagate specific perspectives or information (including mis- and disinformation), to shift conversations at scale, and to mobilize action.

The variety and flexibility of available technologies and platforms in the new media sphere create a context in which information operations methods change rapidly, are adaptable across and between platforms, and are in many ways resilient to disruption efforts. In this way, digital tech and social media provide exploitable features useful for gray zone information operations. The following sections outline crosscutting modalities and these various types of information operations capabilities (affordance manipulation, evasive TTPs, algorithmic manipulation, and multi-platform methods) to provide a comprehensive overview.

6.1 Crosscutting Informational Modalities

Even with the variety of options available to share information, media, and communication, some information practices can be considered crosscutting frameworks for utilizing information operations. Crosscutting modalities of the new media sphere include the use of sensationalism, "seeds of truth," and participatory mediation as frameworks for information propagation. Some derive from broader media contexts such as boosting overall sensationalism, a feature of media that has been increasingly common in news and "news-like" media, particularly with the advent of the 24-hour news cycle and the growth in ability to monitor audience reach of virtually all forms of media. Bigger stories framed in jaw-dropping terms increase reader/viewership.[170] Similarly, "clickbait" headlines—framing intended to be so over-the-top that users feel compelled to click through to read the piece—work in an analogous fashion with even normal, everyday stories ratcheted up into crises, spectacular events, unbelievable statements, or enraging topics.[171] This framing is ubiquitous in digital and social media contexts across the gamut of genres (e.g., news, imitation news, blogs, fiction) and content types (e.g., text, video, podcast, and online radio). As noted by Chen, Conroy, and Rubin, the "willful blurring of the lines between fact and fiction" impacts the veracity of news (information) online, which is "now often driven by the quest for page views," ultimately enabling the spread of "misleading, unverified, and seldom corrected" information.[172]

Several characteristics of the new media sphere have a direct impact across technologies on shaping available information operations capabilities. Interactivity and accessibility of information in digital and social media contexts play an essential role in crosscutting informational practices. Foremost among these in internet cultural practice is creating and sharing information through repetition via participatory mediation, or the interactive production and reuse of media as a mode of communication in digital and social media contexts.[173] A common form of participatory mediation that has developed as part of online culture is the production and sharing of memes. Drawing on the biological associations of Richard Dawkins's original articulation of the concept of memes, the concept of *virality* or *going viral* is used to describe the phenomenon of some memes, or similar cultural phenomena, spreading rapidly and widely across the internet. Some memetic content may "go viral" on its own accord as people share it, while other memetic content can be artificially amplified as part of information operations-driven strategies.[174] For example, many advertisers attempt to make content that will reach viral status as a framework for increasing their brand awareness and sales, an observation particularly true in some influencer marketing efforts. Most important in terms of information operations is that memes and the cultural norms of participatory mediation create a form of interactive, intertextual communication.[175] A variety of texts, ideas, images, sounds, and other media can be interwoven in ways that create new associations, direct conversations, and shape opinions, often drawing together factual and fictional information and deploying divisive concepts through humor.

Two practices within participatory mediation stand out in terms of information operations capabilities: memeification and gamification. *Memeification* is the process of turning a piece of content (e.g., taglines, images, song snippets, cultural icons) into a meme. It also represents a particularly popular form of participatory mediation where users engage with materials, adapt them, and share them, in effect participating in the creation and meaning making of the media itself.[176] This type of participatory mediation is highly popular, leading to the creation of easy-to-use meme generators to create memes specifically. Importantly, this trend also applies to other forms of participatory mediation for social media posts and other digital content. For example, Canva is an app that enables everyday users to create professional looking, high-quality graphic design content and image-based texts for sharing online, offering formats for a variety of social media platform types. Similar types of applications also exist for creating video and audio clips and other forms of media. Along with memeification, gamification is the process of adding "game" elements, such as leaderboards and rewards systems, to non-game environments. *Gamification* has been used in advertising and education as a frame for increasing participatory engagement with brands or learning. Gamification is also increasingly used to spread extreme content and propaganda. For example, memes with images meant to look like game style leaderboards, including "kill counts" of extremist and terrorist attacks, have become increasingly common.[177] And combinations of memeification and gamification potentially create a framework of motivation for participation in extreme information cultures online. This was made clear in the livestreaming first person shooter style footage from the Christchurch attack, combined with the attacker's manifesto and subsequent online extremist community responses further memeifying and gamifying the footage.[178] These kinds of participatory mediation as cultural norms of online environments can help propel information operations materials if those materials are attentive to trends and topics of interest in online and political milieus.

In addition, the accessibility of vast quantities of data and information in the new media sphere provides ample stores of texts, videos, images, sounds, and other content from which to produce participatory media. It enables the linking of disparate topics and the incorporation of esoteric, misleading, or false information in forms that seem realistic.[179] When this occurs accidentally, it is labeled misinformation; when such linkages and incorporations are made intentionally, it is labelled disinformation.[180] Importantly, as more media rooted in mis/disinformation are produced, it increases the available stores of loosely factual or entirely fictional stories and misleading ideas that are available to then be repurposed in further participatory mediation and replication. For example, the QAnon slogan to "do your own research" promotes the idea of sourcing and interpreting news and events by combing the depths of the web and following other "Q" interpreter influencers.[181] From the various interpretations (texts, videos, and podcasts) by Q interpreters, it is clear that QAnon followers "doing their own research" actually engage in participatory mediation, blending information from current events, fringe theories and histories, disproven scientific writings, and a broad range of conspiratorial beliefs.[182] These texts (written, visual, and audio) then become sources for future reproductions, replication, and additional spread of polluted information.

These crosscutting modalities of the new media sphere—including sensationalism and participatory mediation—provide a multiplicity of vulnerabilities for information manipulations and a broad set of utilities for information operations. As IO-driven strategies and campaigns are developed, it is profitable to leverage these types of online cultural norms to activate informational spread through users' networks. When crosscutting modalities are viewed alongside specific information operations capabilities—whether localized, evasive/subversive, or scalar—a broader picture of the utility, potential impacts, and harms of gray zone information operations becomes clearer.

6.2 Localized and Platform-Specific Methods

Localized information operations capabilities are often user-generated modes of employing platform features to achieve specific goals, such as manipulating the spread of information or evading detection. From the evolutionary perspective taken up in this report, some localized IO methods may evolve into capabilities available for use at larger scales (e.g., the evolution of hashtag use and hashtag hijacking as platforms responded to users' preferences for hashtagging posts). These shifts are dependent on changes in IO capabilities and their environments, including users adapting IOs based on their needs and technological changes. Others may remain localized, such as manipulating upvoting on Reddit, because the affordance of upvoting is a structural component of the board and thread format of the platform itself. And new localized IO capabilities may develop as new technologies come into use, for example evasion of content removal on blockchain-based technologies.

Affordance Manipulation

Social media platforms afford a certain feature set that can be manipulated for ulterior motives. For example, on the video-sharing social media platform TikTok, white supremacist extremists make use of popular, community-created hashtags to share videos intended to convey racist messages. Here, users have coopted the #blacklivesmatter hashtag to share videos that promote the view that "black lives don't matter" and similar themes. Accounts like these also use links embedded in their profiles to direct new followers off the platform to external sites that contain additional extremist content, allowing viewers to fall down an extremist content rabbit hole.[183] This affordance manipulation aims to propagate information to target audiences. What follows is a discussion of the concept of an affordance; how affordances are applied in a digital context; the multidirectional nature of digital affordances, whereby software developers design features with an intended set of affordances and users interact with, redefine, or even create new affordances; the ways in which this nature can be manipulated and exploited; and examples of affordance manipulation.

What are affordances and how are they applied in a digital context? The concept of affordances was first introduced by psychologist James J. Gibson in 1979. In its original context of ecology, as proposed by Gibson, an affordance could be thought of as the potential actions provided to a human or animal by environmental cues.[184] For Gibson, affordances were what the environment provided, in a way that made both animal and environment complementary to one another. Gibson tied affordances to perception, noting that affordances could be misperceived, resulting in the person or animal being misled by a perceived affordance (e.g., a demagogue portraying himself as a politician looking to solve society's ills).[185]

In 1988, Donald Norman built upon the concept of affordances through the lens of design and introduced affordances to the field of Human-Computer Interaction (HCI). In the design context, objects should be designed with some clue to their proper usage. This, Norman argued, conveys the purpose of an object without the need for instructions or labels. For example, a doorknob conveys turning of the knob to open a door, and a coin slot conveys to the user that coins fit in the slot in an intuitive way.[186]

Such design decisions are not limited to physical objects. In the context of HCI, digital objects too can have affordances that imply to the user some additional interactive feature set. In the digital sense, a button implies clickability, a menu bar implies a series of dropdown menus with extra options, and a text box conveys that text should be entered in it. Similarly, buttons on social media platforms symbolize a set of possible interactions with the content on the screen, such as liking, sharing, commenting, or retweeting.[187]

Multidirectionality and the creation of new affordances. An affordance, especially in the digital context, is more than just a feature of a particular piece of software or a social networking site. Affordances convey meaning and

have a multidirectional component. This multidirectional component becomes complex, especially where a large community of users is involved, because designers interact with users through designed features; users interact with designed features; and users interact with other users to derive new uses from designed features. In 1991, William Gaver introduced this relational component to the concept of affordances by suggesting that an affordance is shaped by how people interact with it.[188]

This multidirectional relationship was exemplified by Twitter's November 2015 change of its much-loved "favorite" button, which was symbolized by a star, into a "like" button, denoted by a heart. This highlights how developers may create an intended affordance when they design a button, but the user base also influences interactions with the feature, leading the feature to develop unintended and unexpected affordances. Users across the social media platform reacted negatively and lamented the loss of the favorite button. For many users, the star symbol conveyed multiple meanings, separating Twitter from platforms like Instagram and Facebook, which also used the heart symbol for "liking" something. Other users said the new symbol implied liking or loving a post, when they had developed their own usage for the favorite button, such as bookmarking tweets they wanted to return to later. Others were afraid that liking a post with a heart could send the wrong message to the original poster of the tweet. Even one Twitter engineer publicly expressed anguish at the replacement of a value-neutral star icon with a value-loaded heart icon.[189]

Also on Twitter, changes to the platform's newsfeed in early 2016, from a simple reverse-chronological order to an algorithmic order based on popularity of posts, angered many users who enjoyed being able to see their friends' and followed accounts' posts without filtering or rearranging. This highlights how users imagine certain affordances. Users feared that algorithms would favor popular posts from larger accounts and would displace their friends' posts in favor of influencers, thus fundamentally altering the feel and underlying culture of the platform.[190] This led some users to seek ways of keeping the old newsfeed, prompting numerous articles about how to opt out of the change.[191] The change also caused the hashtag *#RIPTwitter* to trend on the platform, suggesting that many users thought the change to an algorithmic system would be devastating to Twitter as a social media site.

Newly emergent affordances are not limited to specific social media platforms. The feature set of social media and the way users interact with those features has created new affordances in the online space writ large that can also make their way into the physical world. One major affordance of social media is the ability to rapidly share information about events as they happen. This includes sharing formal news, informal web postings, or even anecdotal information. The COVID-19 pandemic highlighted how information could rapidly be disseminated through social media, as users shared news stories, debated public health guidelines, and amplified polluted information that consisted of false information and frequently of outright dangerous recommendations. Social media sites cater to and feed a person's desire (both emotional and also chemical) to be liked and to receive attention by including metrics for measuring approval through likes, shares, comments, and retweets.[192] In this way, social media provides not only technical affordances for transmitting information but also social affordances through approval-seeking behavior, which has been observed to result in some of the more negative aspects of social media sharing seen prior to and during the COVID-19 pandemic.[193] In the midst of the pandemic, individuals read and shared information on social media that could have been harmful to their health, either by recommending unsafe treatments, suggesting that the pandemic was a hoax, or advocating for not following public health measures. *Online information produced real world consequences*.

Social media sites enable another form of affordance: mass mobilization. This was witnessed by the world during the 2011 "Arab Spring" uprisings in the Middle East and North Africa region, as protesters used social media sites

to organize protests and demonstrations that ended up displacing some of the world's most enduring autocrats. In the years since, social media has continued to be employed as a powerful mobilization tool. A major way this happens is through the use of trending topics on sites like Twitter to bring attention to protesters' causes. This first gets the attention of the public, then the agenda-setting influence of the mass media.[194] In this way, protesters' message can propagate through multiple mediums and can, in turn, mobilize further individuals to support a cause.

Manipulation and exploitation of affordances. Affordances also can also allow for manipulation or exploitation. An account's credibility, effortless sharing of posts, anonymity, and the incentive structures of social media are just some of the features afforded by social media platforms. These features are intended to improve the user's experience—and, according to former industry insiders, make the experience addictive. Malign actors can take advantage of the affordances offered by these features to conduct IOs.

One way this can take place is through the manipulation of credibility afforded by a particular account's reputation. This credibility affordance can stem from a trusted individual who inadvertently spreads misinformation, such as a friend or family member who garners a level of trust from a user, a prominent influencer's account that amplifies information, or even a coordinated information operation.[195]

The ease of sharing information on social media platforms increases the ease with which false stories or misinformation can spread. Features on social media websites make sharing effortless, requiring minimal input from a user. In essence, users can see something online, then share it almost instantly with all their followers. This ease of sharing with hundreds or thousands of people means that people no longer have to think about what they are sharing, or even if the information is true. Individuals concerned with metrics of their social media accounts are even frequently incentivized to share information that will be attention-grabbing rather than information that is valuable or true. Ease of sharing, a tendency toward sensationalism, and a focus on having a popular account can allow actors to create material specifically for its virality (ability to spread). Sensationalized stories can capture a reader's attention and incentivize them to share with friends while little thought is given to the truth of the material. Actors seeking to set an agenda or to carry out an IO can exploit sensationalism to co-opt users into propagating information for them.[196] When this occurs, it becomes increasingly difficult for social media platforms to discern accounts actively perpetrating an IO from legitimate users spreading viral content.

Another key affordance that can be exploited is anonymity. While social media platforms like Facebook require names instead of usernames, little effort goes into ensuring that people are who they claim to be. Anonymity allows actors to create sockpuppet accounts, which are fake accounts that are meant to appear real to a normal user. These sockpuppet accounts create an authentic looking person who is meant to appear believable and trustworthy. Actors, both state and non-state, can build a believable profile and audience before switching to spreading the intended message of their IO.[197]

The incentive structure of the social web is another affordance that can be manipulated and exploited. Online platforms incentivize maximizing visibility, generating impressions or interactions, and virality. Further, the companies operating these platforms are not always incentivized to take action against misuse of their services. The virality of social media posts and number of eyes looking at each post drives each platform's advertising and revenue model. An IO can be highly profitable for the platform on which it is being conducted! This dynamic can make social media platforms reluctant to clamp down on the sharing of mis/disinformation.[198]

Examples of affordance manipulation. Each social media platform allows different affordances that are platform-specific. IO capabilities intended for one platform may not necessarily be suited for another. Instagram, for example, draws upon image-based content that can encourage the sharing of manipulated images, memes, or other sensationalized content. Facebook incentivizes a closer network of friends and allows for detailed posts and the

creation of private groups for the sharing of information. Twitter incentivizes short posts, often devoid of nuance, that function more as hot takes or pithy quotes about events. This also allows for the sharing of information that is sparse on details, often encouraging rampant speculation by followers.

The TikTok example discussed earlier, in which white supremacist extremists amplified their content through hashtagging and embedding links, is an example of affordance manipulation. At play in this example were affordances specific to TikTok, namely ease of replication and imitation, which is known as *mimesis*. From signup on the platform to daily use, users are incentivized toward virality and toward discovering and/or producing content that reproduces, shares, or imitates other trending content. On TikTok the goal is discovery of new content, as opposed to close interaction with friends (as is Facebook's focus). An actor looking to manipulate TikTok's affordances to amplify content can latch onto a popular hashtag and create content that will be shared with others interested in the same hashtag. Because of this, TikTok was a popular platform to share #BlackLivesMatter and #MeToo posts to reach a wide audience. Actors can co-opt these hashtags to spread their own message by piggybacking on such popularity to propagate information to a wider audience than they would otherwise be able to reach.

The mimetic nature of TikTok also allows for access to a wide audience for other purposes, as when "during the COVID-19 pandemic, Vietnamese officials created a TikTok dance demonstrating the proper way to wash hands and engage in social distancing."[199]

Platforms that enable sharing of information propagate a sense of credibility by showing shared content as though it is posted by the individual sharing the content instead of the original source. This feature of sharing content is one reason that vaccine-hesitant content spreads on Facebook. Researchers noted that the majority of anti-vax posts circulating on social media platforms from February to March 2021 were created by twelve prominent accounts. However, when this content was shared by users to friends or family members, those friends or family members first saw that the post was shared by someone they trusted, making them more receptive to what they were reading. This example highlights how various actors can co-opt regular users to propagate information.[200]

On Twitter, the *trending topics* feature is an important element for keeping up with what is happening on the platform in a particular region and for newsmaking. It can also be gamed by malicious actors. The Atlantic Council's Digital Forensic Research Lab has noted several instances in which a small group of accounts in South Africa have gamed the trending topics feature to make false narratives trend overnight before they were picked up by influential users and the media the following day. In one instance, the hashtag *#RamaphosaResigns* was used by these actors to spread a false narrative that South Africa's Cyril Ramaphosa had resigned as the country's president. Researchers noted that the hashtag began trending overnight, when few users were on Twitter. In total, only around 300 accounts were responsible for starting and amplifying the hashtag. By 5 a.m., the hashtag was trending and was picked up by more prominent users who began using the hashtag to draw attention to their own posts, even if those posts were unrelated. Twelve hours later, the hashtag had gone from 557 mentions to 10,280 mentions. In just twenty-four hours, the hashtag was mentioned 16,730 times. The incident gained media attention as users speculated about what was going on. Meanwhile, Ramaphosa's critics used the hashtag as an opportunity to call for Ramaphosa's actual resignation.[201]

The newsmaking element of Twitter is one multidirectional and emergent affordance that allows users to exploit the platform's incentive and feature structure. The news media follows trending topics as a way of setting the news agenda, which feeds further user content creation. This newsmaking-trending topic feedback loop can be manipulated to hijack the newsmaking process. In one example, automated and fake accounts amplified conspiracy theories about Democratic National Committee staffer Seth Rich having ties to Hillary Clinton's leaked emails during the 2016 election cycle.[202]

These examples—including white supremacists manipulating TikTok hashtags, the sharing of vaccine hesitant content on Facebook, and exploitation of Twitter's trending topics to target South Africa's president—highlight how affordances can be misused. Platform developers create a certain set of affordances, regular users interact with these affordances and sometimes create new or unintended uses. This creative process can allow for manipulation of the platforms in unexpected ways, and actors have already done so as a means of amplifying political narratives and mis/disinformation.

6.3 Evasive and Subversive Methods

Evasive and subversive IO methods are strategically important, and necessary to maintain functional information operations in the new media sphere. This necessity is driven by uptake of digital and social media as well as information and communication technologies and devices that enable surveillance, oversight, and information sharing. These methods enable identity masking, avoidance of detection and subversion of platform and content regulation, as well as strategies that enable cross and multi-platform efforts. Importantly, these tools can be used as protective measures by general users as well as bad actors.

Identity Masking and Anonymity

Identity masking and anonymous use of the web and social media are common practices for a variety of reasons, including preventing harms, cyberbullying, and attacks; conducting open-source intelligence; and conducting nefarious or criminal activity. Often, a mix of technologies and practices are used to secure a user's identity. These include the use of sockpuppet accounts, "burner" devices (smart phones or laptops), virtual private networks (VPNs), and encrypted browsing platforms such as the onion router (TOR). Often these strategies are used together to produce a robust identity masking environment because the practices cover multiple angles of exposure, such as accounts, devices, and IP address/location.

In the frame of gray zone information operations, identity masking and anonymity are often used as part of the methods within planned strategies or campaigns that are designed appear to originate from authentic users. Sockpuppet accounts enable employees of strategic information operations to manage multiple online identities, produce and deploy a wider range of content, engage with identified targets (e.g., topics, accounts, users), and adapt their responses according to their various online personae. Sockpuppet handlers will often utilize these multiple accounts to create dissenting viewpoints and contentious engagement.[203] Sockpuppet accounts are an "analogue" tactic in the sense that they are human-controlled fake accounts.[204] As such, these accounts offer flexibility and creativity compared to software-based fake accounts ("bots") and offer increased ability to evade detection.

Christopher Schwartz and Rebekah Overdorf, researchers studying the use of sockpuppets in electoral campaigns in Kyrgyzstan, describe how the use of sockpuppets has evolved to pose an "adversarial escalation." Formerly, sockpuppets were used as a defensive strategy to support a person or agency, or to evade such platform rules enforcements as bans. However, sockpuppet accounts have evolved into what Schwartz and Overdorf call "infiltrators," utilized as an offensive strategy inclusive of attacking targets.[205] These evolved fake accounts attempt to "assimilate genuine audiences from within."[206]

Additional mechanisms of identity masking include software-based solutions such as virtual private networks that enable users to establish secure connections on public networks and anonymous web-browsing technologies like TOR that mask users' IP addresses and locations while they perform tasks online. The use of VPNs was central to Russian's information operations through the Internet Research Agency, where operators used them to appear to be individuals located in the United States.[207] This marks an evolutionary shift from VPN usage as a primarily defensive information security method to an offensive information manipulation and amplification

one. While TOR browsers are similar to VPNs, in that they mask a user's identity and location, they are primarily engaged to access the dark web, an unindexed bottom layer of the internet "containing content that has been intentionally concealed" (additional details on the dark web follow in the next section).[208] As Kristen Finklea notes: "Anonymizing services such as Tor have been used for legal and illegal activities ranging from maintaining privacy to selling illegal goods—mainly purchased with Bitcoin or other digital currencies. They may be used to circumvent censorship, access blocked content, or maintain the privacy of sensitive communications or business plans."[209] TOR and other browsers that access the dark web enable information manipulation and operations providing access to anonymized spaces. These spaces are often used in the development and deployment of coordinated efforts to disseminate manipulated information and content, ranging from meme warfare to QAnon conspiracy theories.[210] As such, evasive IO methods can work in concert with subversion IO methods.

Avoiding Detection and Subverting Regulation/Terms of Service

For users and information operators seeking to avoid detection, particular locations on the web enable anonymous interactions. Some, like the dark web, are layers of the digital infrastructure. Others, like the Chans (4Chan, 8Chan and its derivative 8Kun, 16Chan, InfinityChan, and Endchan) are platform-based locations favored for their cultures of anonymity by design. The dark web is a subsection of the deep web, a bottom layer of the internet that is not indexed and therefore cannot be reached through mainstream search engines. Navigating the deep and dark web requires specialized browsers that often provide layers of security, including IP masking and multi-relay location masking. The dark web can be used for both offensive and defensive gray zone intelligence operations. It is also used for open-source intelligence research, as well as detection and prevention of cyberthreats.[211] Of current importance for IO efforts is the use of the dark web by non-state violent actors like Daesh, as well as extremist groups like QAnon.

QAnon's use of these fora that facilitate anonymity yielded a particularly high impact because of how members of the movement were able to utilize it as a base for "memetic warfare." Matthew Hannah, an assistant professor of digital humanities at Purdue University, illustrates QAnon's use of these platforms to engage in meme wars:

> Anons also advance particular fronts in the meme wars, announcing specific campaigns in response to current events. For example, following Trump's impeachment, one anon declared a counter-attack. "Must declare a memewar on the Democrats in districts Trump won" the post is titled, "This is part of the 2020 memewar anons." Calling Democratic senators traitors, anons list vulnerable politicians in swing districts with a mission: "Part of the 2020 memewar NEEDS to be strategically targeting these now VERY VULNERABLE democrats with memes so that not only are they voted out of office but democrats lose the House." In another campaign called "VoterID Meme Warfare," anons call for a concerted social media blitz surrounding California primary voting. Claiming that "California has become a hotbed for corruption and crime," anons detail specific objectives including pressuring Democrats to pass voter-ID laws, derailing existing efforts, and shifting media narratives.... While raining hell from the "meme cannons" almost seems whimsical, the aims behind these QAnon war-rooms are clear: control the media narrative and declare information war designed to undermine and derail Democratic political races in an effort to help Trump win reelection. Waging war across social-media platforms with memes and hashtags as ammunition, anons deploy information technology as a weapons system.[212]

This aspect of QAnon's information warfare strategy is particularly important. Memetic warfare can be highly profitable for sowing chaos in the new media sphere and serves as a potential point of exploitation for other gray zone information operators.

As a strategy, memetic warfare developed out of the Chans and through online mobilizations like the GamerGate networked harassment campaign. It is particularly useful for polluting the new media sphere, directing discourse, and propagating messaging. The Chans are notorious for "shit posting" and "edge lord" cultural norms, including trolling, flame baiting, and bullying. 4Chan's image boards /b and /pol, among similar /pol boards on other Chans, have been a primary site of meme production and circulation, followed by 8Chan when moderation increased on 4Chan regarding certain topics and content. 8Chan and its derivative 8kun (which emerged after 8Chan lost its hosting service) are also the birthplace of the QAnon conspiracy theory/movement.[213]

Some of the Chans are accessible on the surface web while others are on the dark web. Chans have the look and feel of older internet forum boards with time-oriented threads and up/down voting used to circulate popular materials.[214] 4Chan's /b board has been responsible for the generation and wide dispersal of some of the most viral memes, and has been an origination site for multiple networked harassment attacks which are coordinated between multiple (often hundreds or thousands) users against identified targets.[215] The Chans are integral components of certain kinds of extremist content on the web, and are especially favored by far right extremists online.[216]

Crucially from the perspective of information operations, the Chans are insular spaces in which successful participation requires enculturation, particularly on the /b and /pol boards, which are particularly relevant for information manipulation.[217] Thus, the Chans are a space most likely to be sources of images or potential stories to be used in production, rather than a site of deployment for operators outside of its own cultural milieu. However, operations conducted over long periods—for example, using sockpuppet accounts—could work their way into Chan culture if the effort was deemed useful, particularly in promoting message propagation outside the Chans.

For users seeking to subvert regulation/restrictive terms of service, the dark web and Chans are good tools, but other alt-tech platforms and services have become increasingly prevalent. These platforms and services are alternatives to mainstream social media and surface web options (e.g., Facebook, Twitter, blogs). Alt-tech platforms often mirror mainstream platforms (e.g., Gab/Parler are Twitter "mirrors") in order to offer alternate sites for users who have grown tired of mainstream platforms' moderation policies.[218] Alt-tech covers a wide variety of platforms and services, including end-to-end encryption (e.g., Element), decentralized networks (e.g., Mastodon or Gab), distributed, peer-to-peer (P2P) file sharing networks (e.g., Skynet), and distributed peer-to-peer (P2P) blockchain protocols (e.g., LBRY, DLive). Some combine social network mirror front-end access with other alt-tech back-end services. For example, Odysee is a web-based front end video streaming platform that mirrors YouTube, but is run on LBRY, a distributed, P2P blockchain protocol that monetizes user-generated content using LBC (LBRY credits), a cryptocurrency within the protocol.[219]

Alt-tech platforms tend to market themselves as zealous protectors of free speech rights. Little to no moderation is a key feature—affordance—of these platforms for many who migrate to them. These sites also often develop as communities for users holding specific political ideologies. This constellation of ideological concentration, contention over speech, and focus on digital freedom make alt-tech platforms sites for exploitation in information operations from a variety of angles. The lack of moderation enables the production, hosting, and circulation of content that would likely be banned on other platforms. Alt-tech sites can thus provide direct access for platform users and also act as hubs for redeploying content and messaging on mainstream platforms to keep it circulating, thus subverting content moderation and platform regulation on mainstream sites. This can reduce content moderation to a game of "whack-a-mole," where removal becomes increasingly difficult for companies as users repost banned content. For example, the Christchurch attack livestream and the film *Plandemic* are banned and removed regularly by mainstream platforms, but users continually repost them (sometimes with slight variations, such as including 10 seconds of static at the beginning, in an attempt to trick automated content moderation).[220]

This capacity, providing a repository for recirculating content, can also be leveraged to enable multi-platform IOs, thus providing tactical support for information operations on a larger scale.

6.4 Scalar and Multi-Platform Methods

This report uses the term *scalar* to indicate cross and multi-platform processes and large-scale operational IO methods used to amplify or suppress information. Scalar information IOs cover a range of user-generated and automated practices intended to achieve specific goals. From the evolutionary perspective employed by this report, scalar methods may have evolved out of localized methods or may have derived from technological changes. Scalar IO methods include algorithmic manipulation as well as tactics such as hashtag hijacking, influencer marketing, and political astroturfing used in cross and multi-platform information operations-driven strategies and campaigns.

Algorithmic Manipulation

As technology has evolved dramatically in the past two decades, so too has artificial intelligence (AI). AI algorithms are now commonplace in our everyday lives. They enable us to quickly search the internet for information, they are used to recommend products we may want to buy, and they are even used to assess creditworthiness. Yet even the most sophisticated algorithms are still produced by humans and are subject to the biases of the humans writing the code, errors in code, or even unintended usage once the algorithms are employed online. Algorithms are value neutral—they can be used for good or ill—which allows for the creation of algorithms that not only help improve our lives but that can be used to mislead the public, to silence public debate, or to openly discriminate against or target certain groups. It is possible for algorithms to be manipulated for various ends, including "gaming the algorithm" to increase the reach of information; "attention hacking" designed to propagate information to other forms of media; automating the process of creating synthetic text for false narratives; and suppressing narratives deemed problematic by privileged actors, such as big tech companies.

Algorithms and Filter Bubbles. One concern that has been expressed concerning algorithmic manipulation is the possible role of algorithms in increasing political polarization by creating so-called filter bubbles. However, Kartik Hosanagar and Alex Miller suggest that a greater level of nuance is needed to understand the role that algorithms may or may not play in political polarization. They highlight three different aspects of the problem to consider: the data used to train algorithms, the logic of the algorithms, and the way people interact with the system.[221] An algorithm is only as good as the data it is trained on; biased or incomplete data can produce biased results. Similarly, algorithms are composed of code written by humans, so if implicit biases from those writing the code are not considered, then the algorithm can produce skewed results. Lastly, those interacting with a system can influence the system. When presented with multiple search results, users choose the site they want to visit. Machine learning algorithms will learn from the sites that users choose to visit, so if users searching for polarizing content consistently visit only sites with specific points of view, the algorithm may come to deprioritize other perspectives, thus potentially limiting other users' ability to be exposed to alternate viewpoints.

However, researchers have shown that the aforementioned self-selection may play a larger role in polarization than do algorithms. On Facebook, users' friends heavily impact what stories they will see and click on; users' self-selected friends play a larger role in reducing the diversity of the newsfeed compared to the effect of the algorithmic newsfeed.[222] This self-selection acts as its own filter bubble, which is shaped independently of AI algorithms. Who a person chooses to be friends with and what television stations they view or newspapers they read can be thought of as analog filter bubbles.

Further research on the effect of algorithms in fragmenting political discourse has shown that in some contexts algorithms have an impact on increasing fragmentation, while in other contexts they can reduce political

fragmentation.[223] Overall, the causes of political polarization are more multifaceted than certain narratives that are overly eager to pin the blame on algorithms suggest.

Attention Hacking. Many actors seek to increase the reach of their message through "attention hacking," which takes advantage of individuals' desire to see sensational content and of content providers' eagerness to provide such content. Sensational content viewership drives engagement metrics on some of the most prominent big tech platforms. A high engagement score in turn prompts recommendation algorithms to promote this content to others, producing an amplification loop that yields yet more viewers to drive further engagement metrics and more recommendations.[224] Attention hacking also aims to capture the attention of individuals with a wide audience, such as influencers or journalists, who then amplify the content further by discussing it with their audiences. For actors employing attention hacking tactics, any coverage is positive coverage. This has been common with far-right groups, who post deliberately controversial content so that when critics or journalists highlight the controversial nature of the content, it unintentionally plays into the hands of the original poster.[225]

Attention hacking is also common in conspiracy theory-oriented circles, as conspiracy theories lend themselves to the sensationalism that feeds attention hacking. These theories can attract attention to the point of going viral. Once recommendation algorithms begin amplifying a theory outside of niche circles due to its high engagement, it is often picked up by the mainstream information environment, further increasing the conspiracy theory's reach to new audiences. This in turn draws more recommendations, as algorithms amplify the now mainstreamed content to broader audiences.[226]

Attention hacking takes advantage not only of individuals' psychological biases but also the incentive structure of the information environment. Neither psychological biases nor information environments encouraging sensationalism are new. What is new, however, is actors' ability to take advantage of technological innovations allowing information to propagate and amplify from a small online community to the mainstream, driven by engagement metrics and recommendations. This innovation allows what would otherwise be considered a fringe community on the Internet to rapidly have its content reach the mainstream, where it can then entice new members. Conspiracy theory communities are aware of this dynamic, and often begin shaping their narrative accordingly from the outset. By creating a sensational yet compelling conspiracy narrative, far right conspiracist actors can effectively anchor their narrative in the minds of those consuming their content.[227] Thus, when a mainstream narrative, such as a fact-checking account, is produced debunking the conspiracy, it may actually *reinforce* the original view and elevate the content to the mainstream.

Gaming Search Engines. One prominent concern about algorithmic manipulation relates to Google's popular search engine, the *de facto* standard for being discoverable on the Internet. Complex algorithms are constantly working behind the scenes to deliver timely and accurate results in response to user search queries. But these algorithms are not perfect—a concern because they shape what users see when they type in a particular search parameter. In 2016, one glaring example of how things can go awry was observed when Google was queried: "Did the Holocaust really happen?" That search query produced shocking results. The top result led to a website titled "Top 10 reasons why the Holocaust didn't happen," which was not the only problematic result. Several of the top ten search results led to neo-Nazi or antisemitic websites, which prompted Google to alter its PageRank algorithm to demote these sites.[228] Yet the incident raised questions about how Holocaust denial sites were chosen by PageRank as the most authoritative sites to provide information about the Holocaust.

Google's search engine is used by 89 percent of the world's Internet users to search the web for information. The process combines complex algorithms and user queries to produce tailored search results.[229] To increase the chances

of appearing in a Google search and thus being found, website administrators engage in search engine optimization (SEO) by including various keywords in the website's code. SEO keywords enable Google's web crawlers to capture and properly categorize a site's content.[230] The algorithms that use this information are complex and constantly changing, prompting an entire industry to form around trying to ensure that a site is search engine optimized to generate maximum traffic by appearing higher in Google's search results.[231]

The SEO industry has produced no shortage of digital marketing strategies and guides on how to optimize a website to appear higher in search results. Google regularly changes its search algorithm to prevent manipulation of its popular search engine, but digital marketing strategists in the SEO industry have not needed to dramatically alter their strategies and guides as a result of Google's changes. Thus, legitimate actors continue to have access to tried and tested SEO strategies to market their businesses and content online. IO actors and those looking to manipulate algorithms can and do also employ these same strategies to drive traffic to their websites, as seen with the example of Holocaust denial sites being the first search results for information about the Holocaust.[232] A Holocaust denial website would only need to optimize itself to appear to Google's web crawlers as though it is sharing legitimate information. This could be accomplished, for example, by keyword spamming, creating web pages that are meant to be indexed by web crawlers but not viewed by visitors, creating fake pages that link to the site, and other techniques aimed at deceiving search engines.[233] *One way this could be used against state actors would be to flood a search engine with web pages purporting to be legitimate websites that actually propagate polluted information about a state's officials, legislative, or foreign policy approaches, or even military deployments*.

Though gaming search engines is a concern, Google has a long history of countering spammers and others who seek to misuse the platform. Only a small fraction of sites that make it to the top ten search results across a variety of popular search queries are manipulated or peddle false or harmful narratives. Getting caught manipulating SEO can result in demotion or even removal from the search engine.[234] Despite this, the gaming of search engines can be a problem in "data voids"—search topics in which there is not enough information to build an extensive list of reputable sites. This allows IO actors to propagate information to users who use a search query that aligns with a data void.[235] Most data voids align with more fringe content, but individuals can then share this information on social media and propagate it beyond the data void.

Automating Synthetic Information Production. In 2020, OpenAI's GPT-3 system was unveiled, which can produce full length articles in partnership with a human editor. The GPT-3 system combines advanced machine learning algorithms and a database of roughly a trillion words of human written prose and is able to respond to prompts from humans. Shortly after going online, GPT-3 had its work published in *The Guardian*, producing articles that humans could not tell were written by an AI, and partook in the Internet pastime of creating memes.[236]

In May 2021, a team at Georgetown University's Center for Security and Emerging Technologies received access to GPT-3 to assess its potential to automate the production of disinformation. The researchers concluded that the system could be used on its own to produce moderate to high-quality written material at scale, though they highlighted that the real strength of the system comes when paired with a skilled operator and an editor. While they noted that GPT-3 would not allow for the full automation of disinformation efforts and was not yet available to the public, the researchers assessed that using the system once it is made available or creating a similar system was well within the capabilities of state actors like China and Russia.[237]

Big Tech as the Arbiter of Truth. A major concern stemming from increasing reliance on algorithms hinges upon the selectivity with which an algorithm displays some information but not other information. Most algorithms are proprietary, making the systems that employ them opaque to the outside observer. Most users searching for products on a site like Amazon simply see what they typed for their search query (the input of the function) and the

results displayed on their screen (the output of the function). All the complex calculations that happened between the input and the output occur in a metaphorical black box. It is often not possible to understand why some results are shown while others are not. Are there unintended biases in the algorithm? Is there a deliberate bias? Has some information been suppressed while other information is weighed more favorably? Such questions have earned tech companies like Google and Facebook the title "arbiters of truth" for the way their platforms can potentially serve as gatekeepers to what information can and cannot be seen by the public.[238]

The foregoing questions become even bigger concerns when one considers how much political discourse now takes place online. Given the way algorithms can be gamed and manipulated and how platforms can effectively serve as "arbiters of truth," researchers have raised concerns over potential election manipulation that could take place as the result of algorithm misuse by foreign or domestic actors.[239] Dan Jerker B Svantesson and William van Caenegem, law professors at Australia's Bond University, argue that individuals presented with information typically evaluate bias for themselves, but in the online news space it is often tech platforms that use algorithms to weigh what information to show users. If the algorithm were manipulated by a nefarious actor, it could be nearly impossible for the end user to detect the manipulation.[240] Such manipulation could be carried out by state actors, non-state actors, or even insider threats working at the tech company with direct access to the hardware and software running the AI systems.

The efforts of Twitter, YouTube, Facebook, Google, and others to demote and remove "fake news" from their platforms following the 2016 U.S. presidential election are one way algorithms can be used to suppress, as opposed to amplify, information. Yet as Hudson Institute scholar Harold Furchtgott-Roth points out, the concept of removing "fake news" can be problematic, as "one person's 'fake news' is another person's reality, and vice versa."[241] In determining what information is fake and what is not, critics worry that the suppressing of information deemed by tech platforms to be untrue creates implied limits on what constitutes acceptable speech. While free speech is not guaranteed on privately run services like social media platforms, their pervasive role as gatekeepers of public discourse has raised concerns about the effect that content moderation may have on free and open societies.[242] In response to this criticism, tech platforms have shifted somewhat toward an "authentic" versus "inauthentic" content moderation paradigm. In this model, authentic content is shared and promoted by algorithms on social media platforms because it constitutes legitimate use of the platform, while inauthentic content is demoted or removed. Thus, the subject matter of the content is less important than the fact that it is being shared by real users in real conversations with other real users.[243] A concern that remains under this model, however, is that technology platforms still exert institutional power to define what is and is not legitimate, authentic content.[244]

The inconsistent and somewhat ill-defined nature of what may trigger content moderation or outright removal has resulted in numerous folk theories—that is, user-generated theories based on the user's perspective of how a platform works—about the algorithms used by big tech.[245] When content suddenly disappears, confusion sometimes abounds among users, the content author, and sometimes even the platform itself. This is because content is sometimes automatically flagged for removal by an algorithm. This process then requires the content to be reviewed manually by an employee of the platform if the removal is appealed. However, sometimes content suited for the platform is still automatically flagged as inappropriate, leaving users and the content author confused. Another source of confusion stems from content that seems to disappear from public view, known in online communities as *shadowbanning*. This folk theory argues that disappearing content is the result of content being algorithmically demoted, sometimes without clear reason. Shadowbanning makes it harder for content to be discovered by other users, constituting a state that is less than outright banning from the platform but has a similar effect of making the user's content nearly invisible.[246]

While content moderation on big tech platforms has been increasing since the 2016 U.S. presidential election, the COVID-19 pandemic brought redoubled effort to moderate content deemed misleading or dangerous. Following a spike in mis/disinformation and conspiracy theories about COVID-19, tech platforms like Twitter, Facebook, and YouTube began to crack down on the sharing of such material, resulting in a large amount of content removal, account closures, and even the deletion of posts from political figures like Rudy Giuliani and Brazilian President Jair Bolsonaro.[247] Content that contradicts public health recommendations was deleted for being "dangerous" and "misleading," and other content was flagged with links directing users to more authoritative sources, like the Centers for Disease Control and Prevention or the World Health Organization.[248] Facebook also employed an army of fact-checkers to review material posted relating to the pandemic. Material deemed untrue was not immediately taken down, but rather was demoted in users' newsfeeds, which, like shadowbanning, makes the material virtually invisible to other users.[249] As Paul Barrett, deputy director of the NYU Stern Center for Business and Human Rights, concluded: "In other words, the platforms have become arbiters of the truth, at least on medical matters related to the pandemic."[250]

Case Study: Daesh's Use of Social Media and Subsequent Deplatforming

The jihadist militant organization Daesh revolutionized the way militant organizations use the Internet to recruit, solicit support, and disseminate propaganda.[251] Daesh's media strategy was sophisticated and multifaceted, but one of its key components was an enormous social media presence. While Daesh was on numerous platforms and has since evolved its tactics in response to account takedowns, its original platform of choice was Twitter. At its peak in 2014, estimates suggested that there were as many as 46,000 Twitter accounts operated by Daesh and its supporters.[252] While Daesh commanded numerous accounts, a RAND report found that Daesh's opponents actually outnumbered it online by a ten to one margin. However, Daesh accounts and their supporters posted almost 50 percent more content—and, similar to an observation we made earlier in this report about the far right, Daesh's strategy was designed to feed off of attention, positive or negative. The clusters of pro-Daesh "hyperactive users" were often able to take advantage of Twitter's trending topics algorithm to get their hashtags trending, where they could reach a broad audience.[253] Even though pro-Daesh accounts constituted a minority, they were a vocal minority that could produce content rapidly and with numerous interactions, while feeding off the work of Daesh's detractors to increase the militant group's visibility.

Pro-Daesh accounts were also tightly networked, which ultimately made them vulnerable to another type of suppression: mass takedown of accounts by Twitter. Daesh thus became a victim of its own success on social media. Pressure mounted for tech platforms like Twitter to do something about Daesh's use of their services.[254] This prompted successive purges of pro-Daesh accounts from Twitter and other prominent mainstream social media platforms. The group's members and supporters would try to immediately return to the platform when their accounts were banned, only to be banned again, creating somewhat of an online cat-and-mouse game. Eventually, though, Daesh found Twitter too challenging an environment and migrated to Telegram (which also took action against the militant group and its supporters, prompting the platform's own cat-and-mouse game). The group also began to branch out to smaller platforms like TamTam and RocketChat to diversify its online presence, though it still uses Telegram as well. Twitter and Telegram's deplatforming efforts did have the effect of denying Daesh an online safe haven.[255]

Mia Bloom points out that while the deplatforming of Daesh demonstrated the overall value of such efforts, the attempted deplatforming of far-right extremists has been less effective due to the existence of replacement platforms like Gab and 8chan, the gradual mainstreaming of far-right messaging, and platforms like Telegram not enforcing similar bans on far-right extremists.[256]

6.5 Multi-Platform IO Methods

Multi-platform IOs are designed to spread and amplify messaging across a variety of channels, which makes them useful for broad reach and larger scale information operations. Multi-platform IOs are utilized in normal digital and social media practice (e.g., advertising, brand promotion, community/group organizing), so users are accustomed to seeing and engaging with information in this way. This allows information operations structured as multi-platform efforts to seem authentic. IO capabilities common to multi-platform operations include hashtag hijacking, influencer marketing (lifestyle branding and 360-degree marketing), and astroturfing (planned campaigns designed to appear as "grassroots" movements). Each of these is discussed below.

Hashtag Hijacking

The use of hashtags began as a relatively platform-specific tactic with its initial use on Twitter.[257] The development of hashtags is an example of affordance manipulation, as they were first proposed by Chris Messina as a way to more easily connect on the platform, while according to Messina, Twitter itself maintained the attitude that "these things are for nerds. They're never going to catch on."[258] Twitter was ultimately incorrect in its assessment of hashtags, which not only became ubiquitous on the site but spread outward to other platforms such as Facebook and Instagram. Hashtags are now highly prevalent in mainstream culture, with the tactic replicated across most social media platforms, used in marketing and advertising, and becoming a functional search parameter in browsers like Google. The development of the broader digital/social media landscape to incorporate hashtags has enabled hashtag use to undergo a tactical evolution from a localized, platform-specific technique to a scalar, multi-platform technique.

The functionality of hashtags for cross-referencing posts has driven their use as an information operations strategy. This usage regularly utilizes a form of cooptation—hijacking—of existing popular hashtags as a strategy for success. As P.W. Singer and Emerson Brooking note, it is easier to appropriate existing viral (popular) online content rather than make content "go viral."[259] Hashtag hijacking, then, is the tactical deployment of messages and content by piggybacking them on unrelated but very popular hashtags. This tactic is part of a larger strategy called *content laundering*, and has the benefit of rapidly and widely circulating information that would otherwise likely only be seen by a small number of users. Hashtag hijacking has been used by activists, advertisers, trolls, and violent non-state actors. Daesh performed several high-profile hashtag hijacks in 2014-15, including taking over hashtags associated with the World Cup to circulate propaganda and violent content to a massive worldwide audience.[260]

A more recent hashtag hijacking is QAnon's takeover of the SavetheChildren hashtag. In the summer of 2020, QAnon followers determined that Wayfair's prices for cabinets and other items were exorbitantly high, and based on an esoteric reading of Wayfair's website, they circulated theories that Wayfair was in fact trafficking in children.[261] QAnon followers saw high prices on furnishings that had products labeled with girls' names (e.g., the Chelsea cabinet) and launched a digital "research" effort linking the product names to the names of missing children to "expose" the purported child sex trafficking plot. Over the course of days and weeks, #WayfairGate morphed into a hijack of the SavetheChildren hashtag, which was used regularly by international NGO Save the Children to promote its work and fundraise. Posts flooded social media, spreading rapidly through mothers' groups. A series of SavetheChildren protest marches were organized across the United States for July and August, from big demonstrations in large cities to smaller protests in rural towns.[262] The campaign took about a month longer to take root in the UK and EU. While participation numbers are difficult to determine with accuracy, the hashtag hijacking expanded the Q following potentially by hundreds of thousands, and exposed millions to QAnon conspiracy messages and content.[263] Crucial to the success of the SavetheChildren hashtag hijacking campaign was

momfluencers—a shorthand for influencers in online mothers' communities—who became prime propagators of the SavetheChildren campaign, and QAnon materials more broadly.[264]

The SavetheChildren campaign suggests that hashtag hijacking campaigns may be evolving to include both a propagation and mobilization component, meaning that large-scale protests stemming originally from hashtag hijacking may become more common. Should hashtag hijacking campaigns continue to evolve in this way, they could pose an enticing vector of direct exploitation.

Influencer Marketing (Lifestyle Branding and 360 Degree Marketing)

Influencers build networks of followers and have a uniquely persuasive "broadcasting" IO capability that is valuable for spreading information. This is a fundamental aspect of the influencer marketing model, and plays a role in companies' decision to pay influencers to market their brands. This is also why alt-right and identitarian cultures have developed a framework for spreading their information and perspective with individual adherents developing brands as online "political" influencers. These influencers—including Ali Alexander, Lana Lokteff, Henrick Palmgren, Brittney Pettibone, Lauren Southern, and Milo Yiannopoulos, among others—have built a networked online culture that Rebecca Lewis refers to as the "Alternative Influence Network" (AIN).[265] These operators leverage the benefits of influencer models, particularly an increase in persuasive reach through seemingly authentic stories and personal connections with audiences, to spread ideological messages and content. They also leverage personal branding strategies to create marketable personas. As Lewis notes, "Blending the 'glamour' of celebrity with the intimacy of influencer culture … influencers display the way they live their politics as an aspirational brand."[266] In this way, political influencers sell ideology to their audiences in both a metaphorical and literal sense.

Influencer cultures and personal brand marketing are also connected with 360 degree marketing and lifestyle branding models, such that influencers can incorporate product lines and be sponsored by companies as an additional way of monetizing their propaganda production. A highly successful example of this is Alex Jones and his channel *InfoWars*, a massive influencer platform that depends on Jones's persona to spread ideology through sensationalism, conspiracy theories, and manufactured rage, along with nearly any product you (don't really) need. Jones's website, YouTube, and Facebook content received 1.4 million daily views on average in the three weeks prior to his deplatforming.[267]

The AIN has developed as a networked community where influencers support other like-minded influencers through interacting with their various channels, participating on the others' shows and podcasts, creating a self-sustaining multi-nodal web in which audience members can immerse themselves. Rebecca Lewis also described a feedback loop that may drive influencers to deliver even more extreme content over time: "For many of the political influencers in the AIN, the more extremist content they make, the more of an extremist and dedicated audience they build. Such audiences can, in turn, drive political influencers to deliver ever more extreme content."[268] These influencers, much like non-ideological influencers, spread their content across multiple platforms; follow and engage in controversies and sensationalism; and become deft at affordance and algorithmic manipulation, particularly manipulation of SEO rankings. They ultimately deploy multiple types of information operations capabilities in their day-to-day practices.[269]

As noted earlier, influencers act as broadcasters and often spread mis/disinformation and polluted information. Thus, they are exploitable in digital information manipulation campaigns and gray zone IOs. This is an important trend to watch for potential evolution. Indeed, the Internet Research Agency's troll/sockpuppet farms seem to already be leveraging influence networks with some accounts (e.g., the previously described Jenna Abrams account). For example, an influencer supported by an adversary could amplify strategic narratives targeting the U.S. to hundreds of thousands of followers.

Political Astroturfing

Along with influencer marketing, astroturfing is another multi-platform tactic derived from advertising cultures. In it, coordinated and planned information operations are created by companies or political groups, then deployed as if they were grassroots movements.[270] Kovic et al. have described the type of political IOs, attempting to influence political outcomes, discussed in this report as digital astroturfing:

> Digital astroturfing is not limited to U.S. elections. Instances of digital astroturfing have been documented in many countries (Wooley, 2016). Astroturfing efforts can be conducted by outside political actors, such as in the 2017 French election (Ferrara, 2017) or in the 2016 Brexit vote in the United Kingdom (Bastos and Mercea, 2017; Llewellyn et al., 2018), or they can be campaigns of political actors within their own country, such as the systematic digital astroturfing strategy of China (King et al., 2017). Digital astroturfing is also not limited to manually curated sock puppets. For example, many digital astroturfing efforts are conducted with automated bots, whereby computer software impersonates humans by acting and reacting in as "natural" ways as possible (Bessi & Ferrara, 2016; Shao et al., 2017; Wooley, 2016).[271]

These authors also include the Internet Research Agency's campaigns under the rubric of digital astroturfing. Similarly, Farrell and Schneier warn about the dangers of AI and automated digital astroturfing campaigns. They write that "when the floodgates open, democratic speech is in danger of drowning beneath a tide of fake letters and comments, tweets and Facebook posts. The danger isn't just that fake support can be generated for unpopular positions.... It is that public commentary will be completely discredited."[272] The use of digital astroturfing in political IOs is increasing, and moving in two directions: analog (i.e., human-controlled) fake accounts and technologically developed, broad-scale comment generators that can push out millions of posts. Both of these directions represent evolutionary shifts in response to environmental and technological factors. While the overall effect of these developments is yet to be determined, their potential in gray zone information operations should not be underestimated.

Multi-platform efforts and algorithmic manipulation offer sets of IO capabilities that can be applied to large-scale operations. This scalar nature makes them useful for a variety of operators. Viewing both scalar and localized IOs within the context of the crosscutting modalities of the new media ecosystem allows a view of how users and technological developments can shape the emergence and adaptation of IO capabilities in ways that impact gray zone information operations.

6.6 State and Pseudo-State IO Campaigns[273]

This report's evolutionary framework focuses on the IOs that various actors employ, and state actors possess the ability to deploy elaborate and well-resourced IO-driven strategies and campaigns that utilize sophisticated IO methods and capabilities. The IOs of state and pseudo-state actors discussed in this section can also inspire or be adapted by other state actors, non-state actors, or even domestic political actors. After all, actors learn from each other's gray zone IOs, making an understanding of state IO campaigns all the more necessary.

Domestically Targeted State and Pseudo-State Campaigns

In recent years, elections have been a common target of IO efforts. In addition to states interfering in other states' elections, domestic actors also have increasingly adapted the IOs used by adversarial states to carry out IOs in their own countries. A report from Freedom House noted that in 2017 18 different states employed disinformation ahead of elections, sometimes even targeting their own electorates. The goal of these IOs was to manipulate the public

into supporting government policies through astroturfing.[274] Countries carried these IOs out in part through the creation of fake online identities masquerading as real citizens supporting certain government policies. The intent is to make it appear that there is public support when there may in fact be little, and to persuade the audience to adopt the same view.[275] Freedom House researchers found that these IOs have been effectively employed by governments they describe as authoritarian, including by the Philippines, Sudan, Turkey, and Vietnam.[276] These campaigns can mobilize the populace in support of the government's agenda while suppressing opposition to said agenda.

Domestic political actors have employed state-sponsored trolling for various ends. A report by the Institute for the Future's Digital Intelligence Lab noted that "state-sponsored trolling combines several problems that digital rights circles have been viewing in isolation for years—cyberattacks, hacking, invasion of privacy, computational propaganda, disinformation, political bots, and the like—into a larger phenomenon that is in a class by itself."[277] While some of these tactics will be described in more detail in a later section, it is worth noting here that states use mobs of supporters, bots, and individuals employed by the state for the purpose of trolling to harass, threaten, or discredit individuals who threaten the state's hold on power. Notable victims include journalists, academics, activists, and opposition politicians.[278]

One way that states use trolls is known as "patriotic trolling." Such an approach leans upon the assumption that those who support a government's policies are true patriots while those who oppose it or cast it in a negative light are unpatriotic. Some states will thus mobilize followers to attack their opponents. Governments in Turkey and Mexico have utilized armies of bot accounts to bolster their policies, attack opponents, and drown out opposing voices.[279] Another way states use trolls is by taking advantage of fears of algorithmic manipulation and fake content. Because state-sponsored trolls are aware that tech platforms are keen to remove inauthentic content quickly, trolls mass report legitimate accounts controlled by individuals who have been targeted by the state, resulting in the tech platforms potentially removing authentic accounts or demoting content that the state wants suppressed.

State-Specific Campaigns

The following section examines IO campaigns carried out by Russia, China, and Iran. The goal of this section is not to highlight the actors but instead to demonstrate similarities between the IOs employed by each state and how these states have evolved their IOs over time.

Russian Active Measures. Russia has a long history of conducting information operations and propaganda campaigns. During the Cold War, the Soviet Union engaged in "active measures" against the United States aimed at discrediting the Western liberal order, advancing Soviet communism, and deflecting Western criticism of the Soviet Union.[280] In the Soviet Union, propaganda was an art form intended to advance strategic goals. This art form remains in practice by Russia even today.

Bringing active measures into the new media sphere was not without missteps for the Russian government. Russia deployed bots under President Dmitry Medvedev in an attempt to control the domestic political narrative and to frame Russian policies in a positive light. However, Russia's technology and media industries were highly competitive at the time, making the relatively unsophisticated bot army unconvincing in the face of a cadre of seasoned Russian bloggers. The failure prompted significant investment in the development of both bots and trolling capabilities that could operate in a highly competitive environment.[281]

Following the refinement of its IO capabilities in this regard, Russia turned to its so-called near-abroad to test new techniques. Beginning in 2014, Russia deployed active measures in Ukraine's Crimea region. Russian media outlets worked to create an image favorable to Russia's invasion and subsequent annexation of Crimea while bots

amplified this favorable narrative and drowned out opposing viewpoints.[282] Russia then turned its attention to other near-abroad countries like Hungary, Poland, and the Czech Republic, before reaching further afield to the United Kingdom, wielding its increasingly powerful propaganda apparatus to support the Brexit referendum in mid-2016.[283]

This led to the most prominent and closely studied example of Russian active measures, which took aim at the 2016 U.S. presidential election. As laid out in the *Report on the Investigation into Russian Interference in the 2016 Presidential Election* by Special Counsel Robert Mueller, Russia interfered in the 2016 presidential election in a "sweeping and systematic fashion" that included computer system intrusions targeting the Democratic National Committee, dumping of hacked documents on the website WikiLeaks, and influence operations conducted by the Internet Research Agency (IRA).[284] In March 2016, the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) compromised computer systems and email accounts belonging to the Clinton campaign, including that of Clinton's campaign manager John Podesta. One month later, the GRU targeted the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC), stealing hundreds of thousands of documents and emails across all three attacks.[285] These attacks were later investigated and attributed by the cybersecurity and incident response firm CrowdStrike, which named the GRU operation APT 28 or Fancy Bear.[286]

Fancy Bear's hack and exfiltration of documents was not the only operation targeting the DNC during the 2016 election. In fact, a prior breach reported to the DNC by the FBI prompted the CrowdStrike investigation in the first place. CrowdStrike soon discovered that the prior breach was perpetrated by a team from Russia's Foreign Intelligence Service (SVR). This team, named APT 29 or Cozy Bear, had been in the DNC's systems slowly exfiltrating information since at least the summer of 2015.[287] Once the materials obtained by Fancy Bear and Cozy Bear were in Russia's possession, they were given to WikiLeaks, which timed the release of the documents to negatively impact Hillary Clinton's presidential campaign.[288]

Fancy Bear and Cozy Bear both compromised the DNC's systems separately and were seemingly unaware of one another's operations.[289] Indeed, the GRU hacked an already hacked system, one that was having emails slowly stolen by the SVR's operation.[290] Don Smith of the cybersecurity firm SecureWorks assessed that without Fancy Bear's dump of the DNC's emails to WikiLeaks, Cozy Bear's operation likely would not have been disrupted by the CrowdStrike investigation.[291]

In addition to the Fancy Bear and Cozy Bear operations, Russia also conducted a social media influence operation aimed at sowing political and social division in the United States. As laid out in detail in an indictment, the Internet Research Agency (IRA) was primarily responsible for this arm of Russia's IO ahead of the election. The IRA bought political advertisements, created social media posts designed to appear as though they were written by Americans, organized political events, and produced material disparaging Hillary Clinton.[292] To better understand political dynamics in the United States, IRA "specialists" began studying American politics, influential groups, and trends as early as 2014, and the IRA started to purchase political advertisements in 2015, showing the operation's deliberate and methodical preparation.[293]

The content produced by the IRA reportedly reached hundreds of thousands if not millions of individuals, according to data from Facebook and Twitter that is cited in the Mueller report. Prominent examples of the operation's activities include running roughly 3,500 political ads on Facebook, scheduling competing rallies designed to get opposing sides in the same place at the same time, targeting ethnic minority groups to suggest they vote for Jill Stein or stay home entirely, and creating a Twitter account that falsely claimed to be the official account of the Tennessee GOP.[294] The ad campaign conducted on Facebook is believed to have cost around $100,000.[295] The actual impact of Russia's interference in the 2016 presidential election remains difficult to assess.[296]

There are some important aspects to note about the 2016 election interference IO. One key aspect highlighted by Thomas Rid and Ben Buchanan is that this was a multi-faceted operation that employed technology to scale. In that way, the 2016 election IO was a departure from Soviet-era active measures. Second, in another departure, Russia targeted voters directly, as opposed to its more standard targets of politicians and journalists.[297] Third, the main victim of the IO, regardless of the influence on the outcome of the election, was the integrity of, and trust in, democracy. Between the IO's attempts to foment distrust in the process and highly partisan perceptions of subsequent investigations and hearings, Russia's message was amplified. Political polarization seemingly increased as the IO became politicized, and trust in the democratic process was eroded.[298]

Chinese Charm and Suppression Campaigns. The People's Republic of China is also active in the IO space. PRC information operations focus on three lines of effort. The first is suppression of narratives unfriendly to the PRC, as well as domestic dissent. Second, the PRC utilizes charm campaigns to promote its economic interests and to positively frame its relationships with a growing number of markets around the world. Third, PRC IOs attempt to diminish the negative appearance associated with doing business with an authoritarian government.

Starting in 2010, the PRC massively increased its state-run media presence abroad. This resulted in a three-fold increase in the number of China Global Television Network (CGTN; previously known as China Central Television) offices operating in major cities around the world, hiring sprees for the newspaper *China Daily*, and the creation of the *Global Times*, a tabloid intended to reach an English-speaking audience (all three of which are state-owned media outlets). By 2018, the Voice of China had been created with the goal of influencing public opinion aboard. This media outlet combined CGTN, China Radio International, and China National Radio into a single entity in order to maximize the effectiveness of the PRC's international outreach efforts.[299] Such efforts expanded the PRC's ability to produce news reports that could paint the PRC in a positive light.

The expansion of the PRC's media reach did more than allowing PRC to manage its image abroad. It also allowed the PRC to more effectively target foreign audiences by publishing and advertising in other countries' publications as well. In September 2018, for example, *China Daily* purchased a four-page advertisement targeting potential voters in the lead-up to the 2018 U.S. midterm elections in the *Des Moines Register,* aimed at highlighting the damage that a continued trade war with China could inflict on Iowan livelihoods. Rather than taking an aggressive tone, this PRC influence operation highlighted the close economic ties between the state of Iowa and the PRC, the ways farmers benefit from free trade with the PRC, and the potential risks of prolonging the trade war.[300]

The "Great Firewall," an elaborate digital censorship system that blocks access from inside China to a wide range of online information that the PRC deems sensitive or inappropriate for domestic audiences, is another way that the PRC exerts influence over the information environment. As a means of augmenting the Great Firewall, the PRC exerts enormous pressure on tech companies like Google, Facebook, and YouTube, including influencing some of what Google is allowed to show in China, and banning Facebook and YouTube entirely.

In addition, the PRC employs roughly two million people to flood Chinese-run social media platforms in order to drown out or suppress criticism of the PRC. It is estimated that these individuals produce around 450 million posts per year.[301] The PRC could also potentially direct at least some of these resources externally, using them in gray zone provocations against competitors.

The PRC has already begun using IOs as a means of interfering in, rather than simply influencing, other countries' politics. In 2018, the PRC conducted a large-scale IO against neighboring Taiwan, which the PRC sees as an extension of mainland China. This IO was aimed at interfering in the re-election campaign of President Tsai Ing-

wen. The PRC's goal was to see Tsai and her Democratic Progressive Party (DPP) lose the election to the Kuomintang party, which maintains a better relationship with mainland China. The resulting propaganda campaign spanned multiple social media platforms, including Twitter, Facebook, and several chat services.

More recently, the PRC amplified and spread conspiracy theories related to the COVID-19 pandemic. In 2020, Chinese officials created and propagated a conspiracy theory that COVID-19 was manufactured at Fort Detrick, the former home of the U.S. biological weapons program and a major biological defense research installation. The conspiracy theory alleged that COVID-19 was brought to China during the 2019 Military World Games. This conspiracy theory was forged in part to direct attention away from the PRC's mishandling of the early pandemic and from allegations that the PRC could be responsible for a leak of the virus from a lab in Wuhan.[302] This helped fuel further COVID-19 conspiracy theories. The PRC also attempted to encourage and reinforce the suppression (e.g., via big tech) of Wuhan lab leak hypotheses about the origins of COVID-19, which were discussed earlier in this report.

Iran's IO Efforts. Iran is also present in the IO space. Iranian operations have repeatedly flooded social media platforms with propaganda campaigns that targeted Western audiences, were favorable to Iranian interests, and disparaged Israel and Saudi Arabia. More recently, Iran escalated to blatant electoral interference, similar to Russia's efforts.

Iran's state-operated social media accounts date back in some cases to 2011. The accounts were first discovered in 2018, when Facebook announced that it had removed hundreds of accounts from its platforms that were conducting two separate IOs. Twitter and Reddit soon followed suit, banning hundreds of accounts for "coordinated manipulation." A subsequent investigation by the cybersecurity firm FireEye determined that the activity stemmed from an IO that started targeting audiences in the United States, UK, and thirteen other countries in 2017.[303] A 2019 report by Christina Nemr and William Gangware further explains Iranian IO efforts:

> Iranian pages have also found success in generating followers by doctoring memes, often around polarizing topics. One popular page with more than 400,000 likes, titled "No racism no war," photoshopped an image of Tom Hanks by adding a Black Lives Matter slogan to his t-shirt. The image generated 95,000 shares. Since 2011, well-produced, fake BBC Persian videos have been created to cover stories and provide analysis inconsistent with BBC Persian's actual content. These videos are posted to websites that are prominent in search results for BBC Persian. The videos have also been spread through pro-Iranian social media pages.[304]

In 2019, Facebook again removed Iranian accounts from its platform, this time for their connection to amplifying propaganda in the lead-up to the 2016 presidential election. Facebook determined that 92 accounts across Facebook and Instagram targeted U.S., UK, and Saudi audiences using a similar approach to that seen by Russia's IRA operation, such as creating fake accounts designed to increase overall political polarization. The Russian operation had a much greater reach than did this Iranian effort.[305] However, this investigation suggests that the similar tactics from Iran and Russia, which happened in parallel, were learned and adopted independently of each other. This highlights the importance of this study's evolutionary framework: actors not only learn from each other but also learn from their own trial and error.

During the 2020 U.S. presidential election, Iran took an even more active role in electoral interference. One operation used spoofed emails sent directly to voters in Florida, Alaska, and Arizona that claimed to be from the Proud Boys, telling voters to cast their ballots for President Trump or "we will come after you." Within days the emails were debunked and the U.S. intelligence community blamed Iran for the IO. The emails were targeted using stolen voter registration data, marking the first effort by Iran to target the United States with stolen voter

registration information. Thomas Warrick of the Atlantic Council argued that the IO may have been less focused on election interference for the sake of interference, and could instead largely be designed as retaliation for policies and actions that angered the Iranian government.[306]

Amplification and Automation Through Bots

In recent years, bots have been used in greater frequency to amplify online content for both domestic and foreign targeted information operations. The number of bots used to spread polluted information is staggering. Twitter reported taking down 70 million accounts in just two months in 2018. Meanwhile, Facebook removed 583 million accounts in the first three months of 2018 alone.

Given these numbers, there is growing concern about advances in AI that will allow for the deployment of natural language processing (NLP) to complement bot-based campaigns. NLP relies on complex AI in an attempt to replicate how humans understand text and speech, allowing computers to talk and understand language as humans do. Popular voice-activated software like Apple's Siri and Amazon's Alexa use such algorithms to process requests from users. NLP-augmented bots are concerning because their usage will complicate efforts to remove bots from social media platforms by making online posts look and feel more authentic, as though real humans wrote them.[307]

Bots can massively amplify the propagation of information as it traverses the media environment. In fact, bots can be programmed to immediately share or retweet a particular account's material. If enough bots are deployed, a post can almost instantly go viral.[308] Bots can also be used to astroturf and manufacture the appearance of grassroots support for a particular policy.[309] Bots could be used in this context against U.S. military deployments, to make the deployment appear unpopular or to turn the local population against U.S. military personnel.

Bots can act as force multipliers for state and pseudo-state actors. Given the replicability of digital content, it does not cost additional money or time to have a computer program post something thousands of times, thus allowing actors with varying amounts of economic resources to deploy armies of bots cheaply. Once acquired by a threat actor, a bot army is reusable. There is already evidence that bots have been reused for multiple purposes, often to take advantage of one crisis before being repurposed to exploit another. Actors reuse the same bots to target multiple elections.[310] This makes bots a versatile and potent tool for actors in the gray zone that want the greatest return on their investment.

7. Mobilization Repertoires

Mobilization repertoires comprise the IOs that can have material effects on culture, society, economics, and politics. In essence, they are IOs that engage everyday people to mobilize in support of an overall goal. In the new media ecosystem, these action-oriented IOs encompass both online and offline practices. These practices may be knock-on effects, intentional or accidental, from IOs, or they may be specific strategies or desired outcomes of gray zone IOs. As with the emergent "infiltrator" sockpuppet strategies discussed in the previous section, some online IO capabilities are intended to propagate mis/disinformation to produce shifts in attitude with an eye toward shifts in behavior and action. Moreover, like information operations, methods to spur action in the new media ecosystem are often dependent on technological developments and may shift or change accordingly. Given that both online and offline mobilization IOs may be useful to an operation or accidental outcomes, there may exist a series of events intermingling propagation and mobilization over time, blurring definitional lines between the two sets of efforts.

Mobilization repertoires include online actions that cover a range of strategies related to the interactivity of digital and social media, including circulation-based tactics (e.g., interactive circulation, intermediation, and reactive circulation) as well as harassment and suppressive tactics (e.g., doxxing, networked swarms, brigading, and swatting).

They also include offline actions, including demonstrations (e.g., protests, movements, events) and violence (e.g., inciting violence). Once developed and deployed in quotidian uses, these efforts become exploitable by gray zone operators. Thus, gray zone information operations may lead to what appears to be "grassroots" mobilization (as with astroturfing, which this report has described previously) that has been manipulated by outside actors. Moreover, outside actors may piggyback on existing mobilized movements (or movements with a potential to mobilize) in an effort to manipulate the mobilization to advance their own aims.

For example, it is now clear that Russian information operations, including the Internet Research Agency, staged a long-term campaign preceding the 2016 U.S. presidential elections which targeted racial divisions in the United States as a primary modality of sowing distrust and division. Between 2015 and the 2020 presidential election, this operation attempted to leverage the Black Lives Matter movement, anti-Muslim movements, and other existing movements. A particular mobilization tactic Russian operatives used was to create fake protest groups to organize "events" for demonstrations, protests, or marches for both sides of an issue (e.g., pro/anti-BLM, pro/anti-immigrant rights). In some cases, the demonstrators at the two Russia-instigated events would clash in the streets.[311] An analysis of Russia's efforts to coopt existing social movements that appeared in the *Washington Post* noted that the Kremlin's "attempts to hijack movements such as Occupy Wall Street and the Standing Rock protests against the Dakota Access pipeline indicate that the Kremlin can skillfully reframe social protests to increase mistrust between U.S. citizens and their government."[312]

7.1 Online Actions

Multiple online action methods rely on the interactivity of the new media ecosystem as a primary catalyst. The affordances of interactivity enable online "actions," such as sharing posts and content, clicking links, researching issues depicted in manipulated information (e.g., "doing your own research"), buying suggested products, making derivative content, and responding to posts. These types of online actions also have an amplifying effect in terms of propagating narratives, content, and dissension. Thus, online actions should be considered a primary aim of mobilization in new media sphere information operations in the gray zone. These types of actions may also lead to offline mobilizations, such as demonstrations and protests, voting and electoral actions, and interactions with government officials (e.g., petitioning, calling politicians, attendance and speaking at school board meetings). They can even build to the point of participation, either intentional or unwitting, in violent action—as with the January 6 Capitol attack.

Participation in online action may benefit from a psychological effect, the *foot-in-the-door phenomenon*, wherein individuals who are asked to participate in small ways initially are more likely to participate in more in-depth ways in subsequent interactions.[313] Nicholas Gueguen explains the phenomenon:

> It was observed that accepting a simple initial request predisposes in a positive way a subject to accept a subsequent request asking for a greater effort. Our experience shows that the "foot-in-the-door" technique can be transposed to situations in which the interactions occur by e-mail. Earlier studies have shown that the physical presence of the demanding person is not necessary to guarantee the compliance to the request. It appears now that this presence not even necessitates a synchronous communication between the applicant and the target of his request. This "electronic foot-in-the door" turns out as effective as in a situation where the interaction is synchronous (face-to-face or by phone).[314]

Such compliance predisposition can be exploited via social media IOs. For example, initial reading, liking, or sharing of posts could potentially work as an initial compliance-gaining action leading to higher impact online and offline actions.

Indeed, initial online interactions—sharing, liking, reposting, and commenting—represent a form of interactive circulation of content, narratives, and manipulated information. Such interactive circulation may be organic, relatively speaking: General users in target environments have seen and interacted with materials from or related to an IO. The circulation may also be manufactured in the sense that a group of information operators may strategically act through fake accounts or utilize a contingent of bots to interact with materials from or related to an IO. Other frameworks for manipulating interactive circulation processes include *intermediation* and *reactive circulation*.

This graphic illustrates how the OK symbol had purportedly been appropriated as a symbol of white power.

Intermediation is the process of cross-linking or blending symbols, images, or narratives for the purpose of coopting their meaning. An example of this is hashtag hijacking (detailed previously), but it also occurs with media content and cultural symbols. Two infamous examples are the cooptation of the Pepe the Frog image and the OK hand symbol by online alt-right and far right cultures. This intermediation of previously popular and iconic images and symbols, converted to represent discriminatory new meanings, was achieved through coordinated (i.e., networked) digital campaigns with the intention of "infecting" the image or symbol to "trigger" (disturb or upset) "normies" (everyday people) and leftists.[315] In these campaigns, Pepe the Frog memes were generated to represent a variety of characterizations from across the spectrum of extreme beliefs (e.g., male supremacism, white supremacism, neo-Nazism, antisemitism). The appropriation of the OK hand gesture is somewhat more complicated, seemingly rooted in a campaign to first fool and then delegitimize mainstream media reporting.[316] The hoax claim being made (e.g., on 4chan) was that the gesture was designed to stand for white power, as illustrated in the accompanying graphic. As extreme Pepe memes and pictures of white youths flashing OK signs continued to be traded, they escaped their origins in online Chan cultures and moved into mainstream digital and social media contexts. Creators/circulators and campaign participants enjoyed their "lulz" (mocking humor at the expense of normies) as people reacted with horror, disgust, anger, and fear. This reaction was the goal of the campaigns, with digital extremist cultures winning in this bit of the culture war.

The ongoing reaction to these coopted symbols (reactive circulation) is the second stage of mobilization in response to such digital and social media campaigns. It includes online, and in some cases offline, action. Recently, a contestant on the game show *Jeopardy* made what many audience members—apparently now highly sensitized to the ostensible white power cooptation of the OK symbol—thought was a "racist hand gesture" during the airing of the show. People took screen captures and shared video of the moment, castigating the show and broadcast company. The contestant did not, in fact, flash a white power symbol.

A more dramatic example of audience reaction to this purported white power symbol is the story of Emmanuel Cafferty. Cafferty, a San Diego Gas and Electric employee, was driving his company truck, arm out the window

and in the midst of cracking his knuckles, when another driver snapped a picture. The stranger posted the image on social media, claiming Cafferty was flashing a white supremacist hand gesture. The post quickly went viral. Twitter users demanded his termination. Despite Cafferty being Mexican-American and vehemently denying all accusations of white supremacy, or even knowing that they supposedly favored a specific hand gesture, he was fired.

When Cafferty's side of the story came to light, his accuser deleted both the original post and entire Twitter account. A petition on the popular site Change.org asked San Diego Gas and Electric to reinstate Cafferty, while on the fundraising site GoFundMe money was raised so he could sue his former employer for wrongful termination. These examples illustrate how planned campaigns to infect information—the pollution of a cultural symbol—can mobilize action online and offline, with increasing effects over time. People unaware the new meaning of the symbol (which, in the case of the OK sign, was a hoax meaning) could have the course of their lives changed by purported association with it.

This image of Emmanuel Cafferty outraged thousands of Twitter users who believed he was forming a gesture of hate instead of casually cracking his knuckles.

These circulation-based IOs—interactivity, intermediation, and reactive circulation—are common practices rooted in the functions of digital and social media. As such, they are exploitable by information operators in the gray zone. Properly targeted deployments of manipulated information can spread widely, impact large audiences, and mobilize a variety of actions.

Suppressive IOs

Along with online mobilization, there are suppression efforts developed by users and exploited by outside actors useful to suppress certain information and silence certain users. Suppression is important to understand within the framework of online mobilization. Even if they are not used directly by information operators, they are very likely outcomes of divisive information manipulation campaigns which may ultimately work in support of gray zone information operations' success. These efforts include online harassment, doxxing, networked swarms (large-scale harassment campaigns), brigading, and swatting. These measures can be used in localized ways against individuals or on specific platforms. They can also be used or leveraged for largescale operations, usually in coordination with multi-platform efforts. The specific efforts used in both localized and scalar mobilization are described in detail in the remainder of this section.

Harassment. Harassment has become a norm across the internet. A 2019 UNICEF poll, for example, found that one-third of young people across 30 countries had been the victim of online bullying.[317] Over a quarter of Canada's 35.6 million internet users reported being harassed on social media.[318] A quarter of internet users surveyed in 2021 reported experiencing "physical threats, stalking, sexual harassment, or sustained harassment," up from eighteen percent in 2017.[319]

Severe online harassment tactics began to move away from the fringes of the internet and into the mainstream in 2013 and 2014, based on several high-profile incident. These incidents include doxxing, a term derived from the

practice of releasing documents or "docs" containing personal information about a target, which has been part of the internet since the 1990s.[320] In the early to mid-2010s the practice gained a sort of popularity as instances of doxxing went viral.[321]

Harassment on message boards, threats to a person's physical safety, and doxxing have all evolved to remain effective in a changing the digital landscape. A variety of actors across the political spectrum have employed these tactics to harass and suppress those with whom they disagree.

Targeting. Targeting is the direct harassment of individuals or groups, often originating in internet campaigns. Russian IOs using targeting have focused on both Canadian Armed Forces (CAF) and NATO forces, particularly those deployed to Latvia. Polluted information has claimed, for example, that CAF personnel are taking advantage of the Latvian government's money, and has depicted them as drunks and litterers. In 2017, a Russian-language pet-lover's page posted photos of trash, including empty water bottles and military rations, claiming they were left behind by CAF and NATO troops after an exercise.[322] Mainstream Latvian media outlets picked up the story without checking its veracity, propagating the information further and giving it more credence. The *National Post* found that the pictures of litter had actually been taken *prior* to the arrival of CAF personnel in Latvia. Also in 2017, a Latvian woman posted on Facebook about a conversation she had with a taxi driver, who told her that CAF and NATO forces were residing in luxury apartments paid for by the Latvian government.[323] This example illustrates how, once polluted information is introduced, it can be spread in a number of ways and take different forms and mediums—including not only being spread digitally, but also by word-of-mouth.

In November 2017, photos showing men in uniform buying large amounts of beer from Latvian shops were shared and spread online. The story claimed that the photos depicted CAF personnel. In fact, the photos depicted U.S. troops buying beer, and they had been taken three years earlier.[324] In 2017, a Russian-language blog published an article that called NATO troops stationed in Latvia "weak, p-ssy, gay, losers, [who] couldn't find job in any other field."[325] This IO contributed to a larger strategic narrative about NATO forces questioning their capabilities. Leaders of Baltic states have expressed concern that Russia is trying to provoke NATO troops into behaving in a way that alienates them from the host population and validates these messages.[326] In April 2020, during Exercise Steele Crescendo, the NATO battle group in Latvia was targeted with polluted information related to the COVID-19 pandemic. False reports spread by several media outlets claimed that there were high levels of infection among NATO troops in Camp Adazi, a NATO base used by Latvian Battle Group forces, including Canadians and Americans. These reports surfaced shortly before an exercise that took soldiers outside the camp and into local areas.[327] The Latvian government began dispelling the rumors within a matter of hours.

Many of the targeted IOs discussed here began in early 2017, as the United States deployed 3,000 troops to Poland. This represented one of the largest post-Cold War American military deployments to Europe as part of NATO's Operation Enhanced Forward Presence. The number of Russian-influenced IOs targeting NATO troops likely increased at this time as a result of that deployment. The U.S., U.S. allies, and NATO should consequently expect the use of polluted information and other forms of information warfare to increase before, during, and after a major deployment, redeployment, or exercise.

Networked Swarms. Swarming is a tactic wherein social media users target individual accounts and hashtags online to harass other users or spread harmful misinformation. Swarms can be dangerous not only for their attacks on individuals but also for their manipulation of conversations online. Recently anti-vaxxers have used social media to harass healthcare workers and overwhelm hashtags with misinformation. Dr. Zubin Damania created the hashtag #DoctorsSpeakUp to try to combat anti-vaccine misinformation online after seeing Dr. Nicole Baldwin

receive death threats for making a video in support of vaccines.[328] The hashtag, however, was commandeered by anti-vaxxers, who used it in posts such as "When will #DoctorsSpeakUp that vaccines harm and kill children?" and "Why won't #DoctorsSpeakUp that vaccines harm many of their patients?"[329] Renée DiResta, a researcher at Stanford, commented on anti-vaxxers' use of swarming tactics: "They're very effectively able to deploy a brigade to flood the comments, or flood the hashtag making it look like the vast majority of public opinion feels a certain way. It's to create the perception that there are very large groups of people who distrust vaccines."[330]

In the future, it is possible that swarming could be used to try to deny the public vital information in a crisis or to amplify a false message that drowns out legitimate communications. An IO accompanying a major armed conflict could be used to flood social media with false information with the intent of preventing the public from having any idea about what was happening.

Brigading. Brigading is another form of harassment that resembles swarming but typically involves a specific, targeted action. It originates from the online forum Reddit. On Reddit, users from one subreddit, a forum dedicated to a particular topic, would work as a group to "downvote" postings on another subreddit, which would result in the targeted subreddit reaching fewer users' feeds and effectively censoring it.[331] Brigading has since been used on other platforms, and includes all activity done with the intention of manipulating the popularity of online content. This may include mass retweeting or liking a post as a means of making content more visible, and also includes making content appear to be less popular, such as mass commenting with negative comments to make the post appear controversial.[332] Mass reporting is another form of brigading wherein a group reports the posts or account of a social media user they wish to attack, often triggering the platform to disable or remove the targeted account until the reports can be reviewed.[333]

Swatting. Swatting is a form of harassment that became popular among internet communities to harass and threaten the lives of targets. In a swatting event, a harasser calls a law enforcement agency and reports a fictitious threat, such as a bomb or hostage situation, at the home or workplace of their target, which can result in a SWAT team or similar emergency response being dispatched to the location. This tactic is far from harmless, and has resulted in the death of several targets.

Around 2011, swatting became a tool of political harassment when conservative bloggers became the target of these attacks.[334] Since then, swatting has become a tool of ideological extremists to harass and threaten those who disagree with them. One prolific "swatter" was recently sentenced for his targeting of minorities and journalists. John Cameron Denton, a former Atomwaffen Division leader in Texas, received a prison sentence in May 2021 for his role in multiple instances of swatting.[335] He "carefully chose" targets based on their identities, including a historically black church, an Islamic center, journalists with whom he disagreed, and members of various minority groups across the country.[336] Denton participated in swatting attacks on 134 locations, using false claims of hostages, pipe bombs, and other violent occurrences to draw law enforcement responders to the scene.[337]

Thus, swatting gives people the ability to threaten the lives of their chosen targets of harassment.

Geotag squatting. Russia has made use of evolving technology to harass and target voices of dissent. When dissident Alexey Navalny was due to return to Russia from Germany on January 17, 2021, certain hashtags and locations on Instagram were flooded with pictures of human faces that appeared to have been created using a generative adversarial network, a way of using an AI to generate fake faces.[338] These posts saturated the platform that many of Navalny's supporters were using to organize, making it difficult for protesters to find authentic posts. This tactic, called *geotag squatting*, employs principles of brigading but has evolved into a more complex method. These accounts, seemingly of real, untrackable faces, were all posting from Red Square, calling for opposition to a rally,

but never specifying a time or location.[339] Some observers perceived this as a tactic designed to draw protesters away from a previously agreed-upon protesting location.

Suppressive efforts in the new media sphere provide benefits for information operators in the gray zone both directly and indirectly. Suppressive tools provide mechanisms of action and forms of individual and collective mobilization that have concrete material effects on targets, from individuals to states.

7.2 Offline Action

Offline mobilizations are often associated with social movement organizing and activism. As this report showed, social media was utilized as an organizing tool for mobilizing multi-country pro-democracy protests across several Middle Eastern countries in 2011 during the Arab Spring. While these technological organizing methods were not the sole modality of mobilization, their use as a "new" tool for activism was cemented by the media coverage of the protests. Since the Arab Spring uprisings, multiple other activist movements have used social media organizing as a framework for drawing public and financial support, as well as bringing people to the streets. In the remainder of the 2010s, these efforts were used in support of the Occupy Wall Street and anti-austerity movements, as well as feminist and anti-racist movements, culminating in online mobilizations that converted to full blown protest movements such as #MeToo and Black Lives Matter.[340] Each successive use of digital and social media for a mobilization spurred evolution of methods and tools as interested actors learned from that mobilization.

Indeed, activist groups and social movement participants look to other movements' actions when developing their own strategies. A recent example of this is the migration of utilizing umbrellas to ward off rubber bullets and smoke canisters, originally used in the Hong Kong pro-democracy protests in 2019, then used in the U.S. in ongoing protests in Portland, Oregon. In Portland, additional tools were developed by activists using everyday items such as garbage cans to make shielding for protection against anti-crowd and dispersal technologies used by the police. The activists created workshops and training to assist each other in creating gear, while street medics set up tables and tents offering services to activists and journalists covering the protests.[341]

As the Portland protests stretched from days into weeks, new contingents of activists mobilized, including the "Wall of Moms," a group of mothers who began going to the protests and standing between the lines of police and activists to show their support for the protests and to provide a human wall of protection.[342] After the Wall of Moms, a new group emerged called the "Leaf Blower Dads," which similarly joined the protests to provide a protective function for activists by using gas-powered leaf blowers.[343] The moms and the dads groups incorporated two types of tools, one a longstanding historical repertoire and the other newer. The longstanding historical tactic is the utilization of parental identity as a source of public political voice, which has been used often by mothers to protest government (in)action. The newer tactic, the use of leaf blowers, seems to at least be partially inspired by the Hong Kong protests' use of easily accessible, everyday items as protective gear. A crucially important outcome of the Wall of Moms tactic in particular was that as media reported on the mothers' mobilization, and the stories spread across social media, other mothers in multiple places in the United States began forming Wall of Moms chapters in their local communities. These examples show how IOs and the methods they use can emerge, migrate, and evolve, sometimes very rapidly.

A major reason that Portland is a prime site for the development and evolution of offline action is its ongoing role as a site of contestation between political poles. Portland has regularly experienced street fighting along with other clashes.[344] Ongoing mobilizations necessitate participants' attention to and development of offline actions. Such techniques are reported widely by the media, thus making them more exploitable by others (i.e., aiding their evolutionary function). The remainder of this section outlines several examples of offline action efforts.

Examples of Offline Action

One of the most important goals for actors conducting an IO is to create some offline change in behavior, to produce a mobilizing effect. Offline action can be aimed at getting people to go out and do a set action, such as attending mass protests or voting a certain way. Conversely, these actions can be aimed at getting people to *not* do something, like the Internet Research Agency's attempts to get people to stay home from the 2016 U.S. presidential election. *Plandemic* is an example of how offline action can be aimed at mobilizing a population to varying ends.

The "Plandemic"

The COVID-19 pandemic spawned numerous conspiracy theories. Prominent theories often linked the coronavirus to other popular conspiracy theories, such as those concerning 5G cell phone networks. COVID-19 conspiracy theorists received a major boon on May 4, 2020, when a 26-minute "documentary" titled *Plandemic: The Hidden Agenda Behind Covid-19* was released on over several social media platforms. The video paints the COVID-19 pandemic as a nefarious plot by elites, and was rife with unfounded claims.[345] These claims included the assertion that if a person was exposed to COVID-19, mask-wearing would "activate" the virus, prompting fears that mask wearing could actually make people get sick. Another claim was that "healing microbes" could be found in the ocean, which would cure those infected with COVID-19.

The video went viral, receiving 8 million views within the first week of its release.[346] The video faced significant criticism and was soon removed from major social media platforms. However, this deplatforming was anticipated by those sharing it, and potentially boosted interest in *Plandemic*. This, as the Atlantic Council's Digital Forensic Research Lab notes, is known as the "Streisand effect," whereby suppressing content online can make it spread more rapidly, similar to how the banning of certain books may increase readership.[347] The video was quickly reposted on alt-tech platforms like BitChute.[348]

Despite its eventual debunking and removal from mainstream platforms, *Plandemic* had an impact on the behavior of those who watched it. The "documentary" is believed to have increased vaccine hesitancy and decreased the willingness of viewers to comply with public health measures.[349] *Plandemic* served as a catchy on-ramp for viewers to dive deeper into the interconnected world of conspiracy theories. But the video also spurred participation in the numerous reopening protests during the height of COVID-19 lockdowns. Some of the protesters were mobilized by their belief that the lockdowns were a nefarious plot, prompting some protesters to attempt to storm government buildings.[350] In addition to promoting vaccine hesitancy, COVID-19-related conspiracy theories have also mobilized individual instances of violence, such as when a man hijacked a train at the Port of Los Angeles to try to ram it into the *USNS Mercy*, a Navy hospital ship deployed to Los Angeles to assist with pandemic response. The hijacker believed that the ship's arrival was part of a "government takeover."[351] Others have burned 5G cell network towers and attacked broadband workers in Canada and the United Kingdom.

Autonomous Zones

An older offline mobilization tactic, one developed by nineteenth century Parisian social movements, has been resurrected in contemporary protest movements since the 2010s. The first modern "autonomous zone" arose in Paris for several months in 1871 and was known as the Paris Commune (additional communes also arose but were quickly put down in other French cities at the time). This tactic has been used in multiple locations since the fall of the Paris Commune.

However, the use of autonomous zones has been increasing since the 2010s. These zones have been employed by various activist movements globally, with different strategies related to localized issues and political contexts.

Perhaps the most well-known recent use of this effort in the North American context was its heavy use across the United States during the height of the Occupy Wall Street movement. Occupy began in Manhattan in September 2011, when activists gathered in and took over Zuccotti Park, "occupying" it for around 60 days. As the movement spread across the United States and globally, it was propagated by social media hashtags, and a variety of public spaces saw the erection of similar camps. These autonomous zones were characterized by decentralized leadership.

The autonomous zone tactic featured prominently amid the unrest that gripped the United States in 2020. On June 8, 2020, ongoing street violence and political pressure led the Seattle Police Department to withdraw from its East Precinct, allowing protesters to occupy the building and establish the Capitol Hill Autonomous Zone (CHAZ).[352] CHAZ was marred by violence in the absence of law enforcement. While its most visible areas were home to murals and community gardens, two teenagers were murdered just blocks away. In total, four people were shot with firearms in CHAZ during its short existence.[353] In addition to these incidents, a rape, arson, and burglary ultimately drew Seattle police back to the zone on July 1, spelling a quick end to CHAZ.

However, CHAZ's short life did not stop it from serving as an inspiration for "activists across the U.S."[354] The PKAZ (Patrik Kimmons Autonomous Zone) popped up in Portland on June 18, 2020, but was dismantled several hours later. On June 22 the BHAZ (Black House Autonomous Zone) was cordoned off by activists in Washington, D.C.'s Lafayette Square; it was also dismantled quickly.

A number of other offline tactics, including black bloc and dearresting tactics, will be involved in establishment of autonomous zones. These tactics are also subject to evolutionary learning.

Mobilization to Violence

The shift from offline mobilization to action into mobilization to violence can be exploited and encouraged, or even incited as part of gray zone IOs. Peaceful protests can be leveraged (by infiltrators or others) to spur increasing violence and generate narratives of institutional and social breakdown in the target.

Generating mobilization to violence in the new media sphere may include, but does not require, direct incitement. Propagating information framed in terms of an existential threat to an in-group (e.g., national, religious, class) identity is a primary mode of information manipulation to mobilize division, anger, and ultimately action. This modality is often used by extremist influencers and group leaders to promote group cohesion (in-group versus out-group) and action.[355] Information framing in a polarized media environment can be exploited to incite and plan violent mobilization on a wider, networked scale. This occurred prior to the Capitol insurrection of January 6, 2021.

This report will not go into detail about the Capitol insurrection, a series of events that have the somewhat paradoxical distinction of having been simultaneously discussed *ad nauseum* yet at the same time understudied in key respects. Further, as we finalize this report, the United States House Select Committee on the January 6 Attack is shifting into high gear in its own investigation of the events. However, from what this report has already covered, a few aspects of the January 6 attack on the Capitol should be clear:

1) The Capitol attack should not be understood in isolation from other mobilizations that occurred throughout the course of 2020-21. Whether other mobilizations (anti-lockdown, racial justice, antifascist and anarchist) that occurred during that period can be seen as ideologically aligned with or in opposition to the January 6 mobilization, this report's evolutionary framework makes clear that the various architects of the January 6 attack watched these mobilizations closely and learned from them.

2) Online mobilizations were extremely important to the massive protest turnout that occurred on January 6 and also the attack on the Capitol. This report has extensively outlined a large number of methods and

capabilities that evolved over time to propagate information (e.g., data points suggesting a stolen election) and also to mobilize an audience from a digital space to a physical place.

3) In the current politicized environment, the January 6 mobilization will not be the last mobilization of political significance that intersects in important ways with extremism and extremist movements. This fact makes it all the more important to understand the techniques of propagation and mobilization that are examined in great detail in this report.

8. Implications

The propagation-mobilization framework proposed by this report allows for a rethinking of the strategic and tactical goals of gray zone IOs to amplify or suppress:

- These two impacts, of amplification and suppression, can produce either positive or negative feedback loops. Just as information can rapidly spread, it can also be suppressed by an IO. Similarly, mobilization can take the form of getting individuals to *not* do something, such as persuading them to stay home rather than voting.
- An IO can *suppress* information in order to mobilize a target audience. For example, an extremist online community may try to suppress moderate voices in order to produce a radicalizing effect. Or an IO targeting a state's elections may amplify information about purportedly fraudulent voting machines in an effort to get people to stay home on election day.
- Thus, by selectively controlling information propagation, an adversary's IO could amplify information painting U.S. forces in a negative light while trying to suppress U.S. counter-messaging, in an effort to turn a foreign population against deployed American personnel in-country.

The conceptualization of gray zone operations as focused on propagation avoids the information-disinformation binary that dominates contemporary IO analysis. Though this report does discuss mis/disinformation in certain contexts, the core framework that the report rests on does not. This avoidance of placing mis/disinformation at the heart of our framework is very intentional and based on several factors, including the fact that there has been significant truth decay in the mainstream information sphere. Multiple factors present in the information environment, such as a tendency toward sensationalism, a rush to publish, and societal polarization have produced an erosion of trust in the mainstream media. They have also complicated the question of what is true and what is not. As the mainstream information sphere loses credibility, its counter-propagation power at least somewhat dissipates.

This report, and its propagation-mobilization framework, also highlights how the gap between propagation of information and mobilization to action has shrunk for reasons that are largely technological but also cultural. This makes it easier for a wide variety of actors, both benign and malign, to mobilize audiences at a distance and at scale:

- Simply put, the social media environment has hastened the connection between the propagation of ideas and mobilization to action. There are both advantages and disadvantages to this dynamic, but one distinct disadvantage is that people may mobilize with demands before the facts have become perfectly clear. Just ask Emmanuel Cafferty, who was summarily fired after he was accused of making a hand gesture that he didn't make, which Twitter users thought possessed a meaning that it did not have.
- Individuals can come across information from a source online that, through the distinct features of social media, they have come to implicitly trust. This can be a celebrity, friends or family members, or someone who falls into that dubious category of extremely online persons known as *influencers*. As such,

the individuals who come across this information can internalize it and alter their behavior as a result. For example, a video like *Plandemic* can cause people to protest COVID-19 lockdowns or flout public health recommendations (e.g., refuse to get vaccinated, refuse to wear a mask). The consequences are potentially deadly.[356]

- Adversarial IOs have already exploited, and will continue to seek to exploit, this shrinking gap between propagation and mobilization.

The means of propagating information and mobilizing audiences to action are, generally speaking, used by a full range of actors. Thus, when forecasting emerging IO threats, it is necessary to understand that new adversarial IOs and IO methods could easily be adapted from legitimate actors; indeed, adversarial IOs often are. Adapting legitimate SEO practices, methods of making memes and viral content, or the methods used by influencers to reach large audiences should therefore be seen as means that could be adapted for an IO.

This report's framework may be applied to anticipate emerging information operation. It behooves professionals utilizing this framework to keep note of IO efforts that have had significant impacts, or where the potential impact was significant. As other actors learn from one another about what works, and what techniques need to be refined, a successful or nearly successful IO is likely to be repeated by a different actor. The actor employing the IO will have noted its effectiveness as well. Therefore, an actor that applies a IOs successfully or quasi-successfully in one arena may apply it elsewhere. If an IO is conducted against an American ally, America should expect that the IO could target Canada, for example, next.

In the context of gray zone IOs, a state's population is a vulnerable point that can be much more easily targeted than in years past due to technological developments. Perhaps the best response to this vulnerability is informing and educating the public on the importance of digital literacy, media literacy, and critical thinking skills. In other words, as IOs become more difficult to detect and disrupt, *addressing the conditions that IOs exploit may be a promising course of action*. Civic education, along with digital and media literacy programs, can help to inoculate the population against more obvious manipulation and address some underlying issues that could be exploited by an IO. Canada has already adopted a digital literacy program aimed at slowing the propagation of IO-generated information following issues of distrust and mis/disinformation tied to the 2019 national elections.[357]

The narrowing propagation-mobilization gap described in this report should also be treated as a force protection issue:

- Increasing instances of extremism in militaries in the West and instances of extremist groups trying to recruit military personnel highlights the danger of possible insider threats that might consume extremist propaganda online and subsequently mobilize in support of a violent non-state actor.[358]
- It is particularly important to ensure that military personnel are trained in digital and media literacy, to recognize extremist IOs, and given concrete recommendations for preventing other military personnel from falling down extremist or conspiracist rabbit holes.

As attention shifts toward combating "fake news" and disinformation, it is likely that gray zone IOs in the new media sphere will lead to collateral damage as technology platforms and the public attempt to disrupt these IOs. Specifically, concerns about disinformation and conspiracy theories will likely result in the suppression of legitimate information as well, as our discussion of the COVID-19 lab leak hypothesis shows. It is thus necessary to exercise caution and some restraint in trying to combat and disrupt a gray zone IO lest the effort unintentionally silence legitimate debate. However, this could become even more of a challenge as IOs potentially begin to look increasingly authentic.

Ultimately, gray zone competition focuses on attacking an enemy nation's will to achieve political goals. The most effective gray zone tool has been IOs targeting societal fractures and confidence in government. In this report, we explored the use of emerging technologies in the gray zone by creating and applying a new framework for understanding gray zone IOs that corrects common misconceptions that cause Western countries to be blindsided. The framework introduced two lines of effort to gray zone attacks: propagation and mobilization, and showed that gray zone IOs can be understood as having one of two impacts on these lines of effort, creating positive or negative feedbacks. In showcasing a variety of IOs to achieve propagation of information and mobilization to action, we hope that this report will help to enable scholars and researchers to build on this approach, increase awareness among technology developers and policymakers of the multiple material effects of the new media ecosystem and information environment, and last but certainly not least, this report is intended for use by practitioners to increase their ability in anticipating and countering a wide spectrum of threats from rival states, non-state actors, and individuals.

Endnotes

1 Sabri Ben-Achour, "Chinese Group Faked Social Media Posts Against a Planned Texas Rare-Earth Metal Plant, Researchers Say," *Marketplace*, June 29, 2022, https://www.marketplace.org/2022/06/29/chinese-group-faked-social-media-posts-against-texas-rare-earth-metal-plant-researchers-say/.

2 Mandiant Threat Intelligence, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance," June 28, 2022, https://www.mandiant.com/resources/dragonbridge-targets-rare-earths-mining-companies.

3 Ibid.

4 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), p. 7.

5 Arthur F. Lykke Jr., ed., *Military Strategy: Theory and Application* (Carlisle, PA: U.S. Army War College, 1998).

6 Aron Nimzowitsch, *My System & Chess Praxis: His Landmark Classics in One Edition* (Alkmaar, The Netherlands: New in Chess, 2016), p. 15.

7 Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (London: Rowman and Littlefield, 2020).

8 The TTP map that follows, and all other explanatory model graphics included in this report (The New Media Sphere, New Media Sphere Circulation Flows, and Information Circulation Characteristics) were created by Ashley A. Mattheis during the course of her work on this project in 2021. Please contact either the creator or Valens Global (info@valensglobal.com) for permission to use graphics appearing in this report.

9 Rid, *Active Measures*, p. 7.

10 For discussion of the internet's evolution from Web 1.0 to Web 2.0 and then to the social web, see Eric Schmidt & Jonathan Rosenberg, *How Google Works* Kindle ed. (New York: Hachette, 2014), locs. 3235-46.

11 Statista, "Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2018 (in Millions)," 2019; Adrienne LaFrance, "The Largest Autocracy on Earth," *The Atlantic*, September 27, 2021.

12 Rid, *Active Measures*, p. 7.

13 For a discussion of early lone plotters' failures, see Emily Hunt, "Virtual Incompetence," *The Weekly Standard*, August 17, 2006.

14 Scott Shane, "Texas Attacker Left Trail of Extremist Ideas on Twitter," *The New York Times*, May 5, 2015.

15 United States Department of Justice, press release, "Ohio Man Sentenced to 20 Years in Prison for Plot to Attack U.S. Government Officers," November 23, 2016.

16 Chip Le Grand, "Seven Years for Terror Teen's Melbourne Bomb Plot," *The Australian* (Australia), December 7, 2016.

17 U.S. Department of Justice, press release, "Two Individuals Charged in Superseding Indictment with Conspiring to Commit Acts of Terrorism Transcending National Boundaries," April 21, 2016; Del Quentin Wilber, "Here's How the FBI Tracked Down a Tech-Savvy Terrorist Recruiter for the Islamic State," *L.A. Times*, April 13, 2017.

18 "Factual Basis," *United States v. Sullivan*, 1:16-cr-05-MR-DLH (W.D. N.C., November 14, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Factual%20Basis.pdf.

19 United States Department of Justice, press release, "New York Man Sentenced to 17 Years in Prison for Attempted Murder of a Federal Officer," April 26, 2018.

20 Sentencing Memorandum, *United States v. Ferizi*, 1:16-cr-042 (E.D. Va., September 23, 2016), https://www.justice.gov/opa/file/896326/download.

21 "U.S. Airmen Terror Attack: Junead Khan Found Guilty," *BBC* (UK), April 1, 2016.

22 Bridget Moreng, "ISIS' Virtual Puppeteers," *Foreign Affairs*, September 21, 2016.

23 Amarnath Amarasingam, "An Interview with Rachid Kassim, Jihadist Orchestrating Attacks in France," *Jihadology*, November 18, 2016, https://jihadology.net/2016/11/18/guest-post-an-interview-with-rachid-kassim-jihadist-orchestrating-attacks-in-france/.

24 Henry Samuel, "Man Held Over Jihadist Murders of French Police Couple After 'DNA Found on Their Computer,'" *The Telegraph* (London), December 11, 2017.

25 Moreng, "ISIS' Virtual Puppeteers."

26 "French Police Arrest Teenager Over 'IS Terror Plot,'" *BBC,* September 14, 2016.

27 "Menace terroriste: le jeune homme arrêté à Clichy a été mis en examen et écroué," *Le Parisien* (France), October 4, 2016, http://www.leparisien.fr/faits-divers/terrorisme-un-homme-soupconne-de-vouloir-commettre-une-attaque-mis-en-examen-et-ecroue-04-10-2016-6175613.php.

28 Romina McGuinness, "French Terror: Man and Pregnant Girlfriend Arrested in France Over Terror Attack Plot," *Express* (U.K.), October 17, 2016.

29 Conor Gaffey, "Notre Dame Gas Plot: Three Women With Suspected ISIS Links Under Investigation," *Newsweek*, September 13, 2016.

30 Soren Seelow, "Sarah Hervouet, 23, Would-Be Martyr [French]," *Le Monde*, October 11, 2016.

31 Caroline Jack, *Lexicon of Lies: Terms for Problematic Information* (New York: Data & Society Research Institute, 2017), p. 6, https://datasociety.net/wp-content/uploads/2017/08/DataAndSociety_LexiconofLies.pdf.

32 John F. Kennedy, "United States Military Academy Commencement Address" (speech, West Point, N.Y., June 6, 1962), https://www.americanrhetoric.com/speeches/jfkwestpointcommencementspeech.htm.

33 Philip Kapusta, "The Gray Zone," *Special Warfare* 28:19-25 (October-December 2015).

34 Ibid.

35 See discussion of these various conceptualizations in Sandor Fabian, "Irregular Versus Conventional Warfare: A Dichotomous Misconception," Modern War Institute, May 14, 2021, https://mwi.usma.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception/.

36 North Atlantic Treaty Organization, press release, "Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales," September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

37 David Carment & Dani Belo, *War's Future: The Risks and Rewards of Gray-Zone Conflict and Hybrid Warfare* (Calgary: Canadian Global Affairs Institute, 2018), p. 2.

38 Jean-Christophe Boucher, *Hybrid Warfare and Civil-Military Relations* (Calgary: Canadian Global Affairs Institute, 2017), p. 1.

39 Nathan P. Freier et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: US Army War College, 2016), pp. 4-5.

40 Ibid., p. 5.

41 Lindsey R. Sheppard & Matthew Conklin, *Warning for the Gray Zone* (Washington, DC: Center for Strategic and International Studies, 2019), p. 4.

42 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND, 2019), p. xi.

43 Scott Haviland, David Cook & Don Newberry Jr., "Into the Gray Zone: Integration of Civil Affairs and Information Operations with Embassies," Association of the United States Army, March 30, 2021, https://www.ausa.org/publications/gray-zone-integration-civil-affairs-and-information-operations-embassies.

44 Ibid.

45 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND, 2019), p. 18.

46 Ibid.

47 Quoted in Lauren Elkins, "The 6th Warfighting Domain," *Over the Horizon*, November 5, 2019, https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.

48 Adam Petrin, *Operationalizing the Gray Zone: A Challenge for Canada* (North York, Ontario: Canadian Forces College, 2019), p. 10, https://www.cfc.forces.gc.ca/259/290/308/305/petrin.pdf.

49 Omer Dostri, "The Reemergence of Gray-Zone Warfare in Modern Conflicts," *Military Review* (January-February 2020).

50 Aiden Hoyle et al., "Gray Matters: Advancing a Psychological Effects-Based Approach to Countering Malign Information Influence," *New Perspectives* 29:144-164 (2021), https://doi.org/10.1177%2F2336825X21995702.

51 *The Conduct of Information Operations* (Washington, DC: U.S. Department of the Army, October 2018), p. 19.

52 Ibid.

53 Aiden Hoyle et al., "Gray Matters: Advancing a Psychological Effects-based Approach to Countering Malign Information Influence," *New Perspectives* 29:144-164 (2021), https://doi.org/10.1177%2F2336825X21995702.

54 *The Conduct of Information Operations*, p. 20.

55 Hoyle et al., "Gray Matters."

56 Rory Cormac & Richard J. Aldrich, "Gray Is the New Black: Covert Action and Implausible Deniability," International Affairs 94:477–94 (2018), https://academic.oup.com/ia/article-pdf/94/3/477/24808421/iiy067.pdf.

57 Thomas Paterson & Lauren Hanley, "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes,'" *Australian Journal of International Affairs* 74:439-454 (2020).

58 Daniel Schiff, Kaylyn Jackson Schiff & Natalia Bueno, "The Liar's Dividend: The Impact of Deepfakes and Fake News on Politician Support and Trust in Media," Georgia Institute of Technology, February, 19, 2021, https://gvu.gatech.edu/research/projects/liars-dividend-impact-deepfakes-and-fake-news-politician-support-and-trust-media.

59 *Threat Report: The State of Influence Operations 2017-2020* (Menlo Park, CA: Facebook, 2021), pp. 3-4, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf.

60 Aiden Hoyle et al., "Gray Matters: Advancing a Psychological Effects-based Approach to Countering Malign Information Influence," *New Perspectives* 29:144-164 (2021), https://doi.org/10.1177%2F2336825X21995702.

61 Jesper Strömbäck, Kajsa Falasca & Sanne Kruikemeier, "The Mix of Media Use Matters: Investigating the Effects of Individual News Repertoires on Offline and Online Political Participation," *Political Communication*, November 2, 2017, https://doi.org/10.1080/10584609.2017.1385549; P.W. Singer & Emerson T. Brooking, *Like War: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt), p. 25.

62 Victor Wiard & David Domingo, "Fragmentation Versus Convergence: University Students in Brussels and the Consumption of TV Series on the Internet," *Participation Journal of Audience and Reception Studies*, May 2016, https://dial.uclouvain.be/pr/boreal/object/boreal%3A216648/datastream/PDF_01/view.

63 Suzy E. Park, *Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues* (Washington, DC: Congressional Research Service, May 30, 2019), https://fas.org/sgp/crs/misc/R45746.pdf.

64 See Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York: New York University Press, 2006), p. 3.

65 Matthew Ingram, "Is Vice Media Really a Unicorn?," *Fortune*, May 5, 2015, https://fortune.com/2015/05/05/vice-media-unicorn/.

66 Ben Collins & Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World," *Daily Beast*, November 3, 2017, https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

67 Ibid.

68 Mirjana Pantic & Ivana Cvetkovic, "Journalism Practice in a Digital Age: Utilization of Social Media in Online News," *American Communication Journal* (2020), pp. 1-12, http://www.ac-journal.org/wp-content/uploads/2020/11/Journalism-Practice-in-a-Digital-Age-Utilization-of-Social-Media-in-Online-News.pdf.

69 Kevin Baron, "How Will Biden's Pentagon Handle Extreme Right-Wing Media?," *Defense One*. January 7, 2021. https://www.defenseone.com/ideas/2021/01/next-extremists-facing-pentagon-right-wing-media/171252/.

70 Maura Conway, Ryan Scrivens & Logan Macnair, *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends* (The Hague: International Centre for Counter-Terrorism, October 2019); Paolo Gerbaudo, "From Cyber-Autonomism to Cyber-Populism: An Ideological History of Digital Activism," *tripleC* 15:2 (2017), pp. 477-489.

71 Deen Freelon, Alice Marwick & Daniel Kreiss, "False Equivalencies: Online Activism from Left to Right," *Science* 369, September 4, 2020, pp. 1-5.

72 Mariah L. Wellman, Ryan Stoldt, Melissa Tully & Brian Ekdale, "Ethics of Authenticity: Social Media Influencers and the Production of Sponsored Content," *Journal of Media Ethics* (2020), pp. 68-82, https://doi.org/10.1080/23736992.2020.1736078.

73 Ryan M. Milner, *World Made Meme: Public Conversations and Participatory Media* (Cambridge, MA: MIT Press, 2016), p. 31.

74 Brandee Johnson, "Influencer Marketing for Lifestyle Brands: A Helpful Guide," Limelight Marketing Blog, n.d., https://limelightmarketing.com/blogs/influencer-marketing-for-lifestyle-brands/; "Why Luxury Brands MUST Go Beyond Digital and Embrace 360-Degree Experience," *AMEInfo.com*, June 7, 2018, https://www.ameinfo.com/lifestyle/why-luxury-brands-must-go-beyond-digital-and-embrace-360-degree-experience/.

75 Rebecca Lewis, "Alternative Influence Networks," *Data and Society*, September 18, 2018, https://datasociety.net/library/alternative-influence/.

76 Rebecca Lewis, "Alternative Influence Networks," *Data and Society*, September 18, 2018, https://datasociety.net/library/alternative-influence/.

77 Alice Marwick & Rebecca Lewis, "Media Manipulation and Disinformation Online," *Data and Society* (2015), May 15, 2017, https://datasociety.net/library/media-manipulation-and-disinfo-online/.

78 Paul Mena, Danielle Barbe & Sylvia Chan-Olmsted, "Misinformation on Instagram: The Impact of Trusted Endorsements on Message Credibility," *Social Media and Society*, April-June 2020, https://doi.org/10.1177%2F2056305120935102.

79 *The Disinformation Dozen Report* (London: Center for Countering Digital Hate, March 24, 2021), https://www.counterhate.com/disinformationdozen.

80 Henry Jenkins, Sam Ford & Joshua Green, *Spreadable Media: Creating Value and Meaning in a Networked Culture* (New York: NYU Press, 2013), pp. 40-45. Also see discussion in Richard Stengel, *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It* (New York: Atlantic Monthly Press, 2019) pp. 1-10.

81 "Global Social Media Stats," *Datareportal.com*, August 2021, https://datareportal.com/social-media-users.

82 "Platforms (Digital Business)," *Gartner Glossary: Information and Technology Glossary*, 2021, https://www.gartner.com/en/information-technology/glossary/platform-digital-business.

83 Whitney Phillips, *The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online*, (New York: Data & Society, May 2018), p. 7.

84 Yariv Tsfati, H. G. Boomgaarden, J. Strömbäck, R. Vliegenthart, A. Damstra and E. Lindgren, "Causes and Consequences of Mainstream Media Dissemination of Fake News: Literature Review and Synthesis," *Annals of the International Communication Association* (2020), p. 157, https://doi.org/10.1080/23808985.2020.1759443.

85 Here, the argument does not refer to the political position or framing of media sources. As such, *reputable media* encompasses media across the political spectrum. *Disreputable media*, in this context, is media that trades in problematic information as its mainstay product (e.g., *The Enquirer*, InfoWars, Health Nut News).

86 Heidi Legg, Joe Kerwin & Grace Greason, *The Fight Against Disinformation in the U.S.: A Landscape Analysis* (Cambridge, MA: Shorenstein Center on Media, Politics, and Public Policy, October 2018), p. 5; Dhavan V. Shah et al. "Revising the Communication Mediation Model for a New Political Communication Ecology," *Human Communication Research* 43 (2017), https://doi.org/10.1111/hcre.12115.

87 David A. Copeland. *The Idea of a Free Press: The Enlightenment and its Unruly Legacy* (Evanston: Northwestern University Press, 2006), pp. 14-15.

88 The lack of a consensus definition is noted in Brent Kitchens, Steven L. Johnson, and Peter Grey, "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption," *MIS Quarterly*, December 2020, p. 1619, http://dx.doi.org/10.25300/MISQ/2020/16371.

89 Ibid., p. 1621; Seth Flaxman, Sharad Goel & Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly*, March 22, 2016, p. 299, https://doi.org/10.1093/poq/nfw006.

90 Brent Kitchens, Steven L. Johnson, and Peter Grey, "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption," *MIS Quarterly*, December 2020, p. 1621; Seth Flaxman, Sharad Goel & Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly*, March 22, 2016, p. 299.

91 Brent Kitchens, Steven L. Johnson, and Peter Grey, "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption," *MIS Quarterly*, December 2020, p. 1622.

92 Seth Flaxman, Sharad Goel & Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly*, March 22, 2016, p. 299.

93 Brent Kitchens, Steven L. Johnson, and Peter Grey, "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption," *MIS Quarterly*, December 2020, p. 1620.

94 Ibid., p. 1642.

95 Alice E. Marwick & danah boyd, *I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience* (New York: Data and Society, July 7, 2010), p. 2.

96 Ibid., p. 9.

97 Ibid., p. 17.

98 Eun-Mee Kim & Jennifer Ihm, "Online News Sharing in the Face of Mixed Audiences: Context Collapse, Homophily, and Types of Social Media," *Journal of Broadcasting and Electronic Media*, December 9, 2020, p. 757, https://doi.org/10.1080/08838151.2020.1835429.

99 George Pearson, "Sources on Social Media: Information Context Collapse and Volume of Content as Predictors of Source Blindness," *New Media and Society* (2021), p. 1182, https://doi.org/10.1177%2F1461444820910505.

100 Hartmut Wessler & Rainer Freudenthaler, as quoted by Ashley A. Mattheis, "Disrupting the Digital Divide: Extremism's Integration of Offline / Online Practice," *Interventionen*, December 14, 2019, p. 12.

101 Barath Ganesh, "The Ungovernability of Digital Hate Culture," *Journal of International Affairs*, December 19, 2018, https://jia.sipa.columbia.edu/ungovernability-digital-hate-culture.

102 Michael Warner, "Publics and Counter Publics," *Public Culture*, Winter 2002, pp. 51-62, https://muse.jhu.edu/article/26277.

103 Lauren Berlant. *The Female Complaint: The Unfinished Business of Sentimentality in American Culture* (Durham, NC: Duke University Press, 2008) p. 10.

104 Ibid., p. viii.

105 Emma Betuel, "Can Masks Spread Conspiracies: Inside the World of QAnon Merch," *Inverse*, November 3, 2020, https://www.inverse.com/culture/qanon-masks.

106 P.W. Singer & Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), p. 162.

107 Ashley A. Mattheis. "Shieldmaidens of Whiteness: (Alt)Maternalism and Women Recruiting for the Far/Alt-Right," *Journal for Deradicalization*, Winter 2018/2019, pp. 150-51, https://journals.sfu.ca/jd/index.php/jd/article/view/177.

108 Ashley A. Mattheis, "Disrupting the Digital Divide: Extremism's Integration of Offline / Online Practice," *Intervetionen*, December 2019, p. 13, https://interventionen.blog/2020/04/21/disrupting-the-digital-divide-extremisms-integration-of-offline-online-practice/.

109 Henry Jenkins, Sam Ford & Joshua Green, *Spreadable Media: Creating Value and Meaning in a Networked Culture* (New York: NYU Press, 2013), p. 2.

110 Ibid., pp. 3-6.

111 Ibid., p. 11.

112 Ibid., pp. 11-12.

113 Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (London: Rowman and Littlefield Publishers, 2020), p. 18.

114 See Charles Tilly, *Regimes and Repertoires* (Chicago: University of Chicago Press, 2006), p. 35.

115 Charles Tilly, as quoted in Veilleux-Lepage, *How Terror Evolves*, p. 18.

116 Veilleux-Lepage, *How Terror Evolves*, p. 21.

117 Ibid., pp. 62-63.

118 Elle Hunt, "Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter," *The Guardian*, March 24, 2016, https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter.

119 Oscar Schwartz, "In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation," *IEEE Spectrum*, November 25, 2019, https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation.

120 Ibid.

121 Nicole Perlroth, "Fake Twitter Followers Become Multimillion-Dollar Business," *New York Times*, April 5, 2013; Josh Constine, "Instagram Caught Selling Ads to Follower-Buying Services it Banned," *TechCrunch*, January 15, 2019, https://techcrunch.com/2019/01/15/dont-buy-instagram-followers/.

122 Ian Carlos Campbell, "Instagram Scammers Figured Out a Way to Get Paid for Banning People," *The Verge*, August 5, 2021, https://www.theverge.com/2021/8/5/22611309/instagram-banned-accounts-business-impersonation. *Bots*, short for robots, are automated programs that perform repetitive tasks and can be designed to mimic the online activity of humans. They may be social media bots that post certain types of informational material on a regular schedule or in response to a user query; they can be web crawlers used by search engines; or they can be used for nefarious purposes to automate authentic-looking social media posts while masquerading as a person. For more information on bots and their varied usage, see "What is a bot? | Bot definition," Cloudflare, n.d., https://www.cloudflare.com/learning/bots/what-is-a-bot/.

123 Henry Jenkins, Sam Ford & Joshua Green, *Spreadable Media: Creating Value and Meaning in a Networked Culture* (New York: NYU Press, 2013), p. 19.

124 Ryan M. Milner, *World Made Meme: Public Conversations and Participatory Media* (Cambridge, MA: MIT Press, 2016), p. 1.

125 Henry Jenkins, Sam Ford & Joshua Green, *Spreadable Media: Creating Value and Meaning in a Networked Culture* (New York: NYU Press, 2013), p. 27; Ryan M. Milner, *World Made Meme: Public Conversations and Participatory Media* (Cambridge, MA: MIT Press, 2016), p. 2.

126 Ryan M. Milner, *World Made Meme: Public Conversations and Participatory Media* (Cambridge, MA: MIT Press, 2016), p. 2.

127 Poppy Noor. "How the Alt-Right Co-opted the OK Hand Sign to Fool the Media," *The Guardian* (London), October 3, 2019, https://www.theguardian.com/world/2019/oct/03/ok-sign-gesture-emoji-rightwing-alt-right.

128 Ashley A. Mattheis, "Beyond the 'LULZ': Memeification as 'Meaningful' Gamification in Far-Right Content," *GNET Insights*, January 18, 2021, https://gnet-research.org/2021/01/18/beyond-the-lulz-memifying-murder-as-meaningful-gamification-in-far-right-content/.

129 Ibid.

130 James Price Dillard & Eugenia Peck, "Affect and Persuasion: Emotional Responses to Public Service Announcements," *Communication Research* (August 2000), p. 461.

131 John T. Cacioppo & Richard E. Petty, "The Elaboration Likelihood Model of Persuasion," *Advances in Consumer Research* (1984), pp. 673-74.

132 Paul Mena, Danielle Barbe & Sylvia Chan-Olmsted, "Misinformation on Instagram: The Impact of Trusted Endorsements on Message Credibility," *Social Media and Society* (April-June 2020), p. 2.

133 Caitlin Dewey, "6 in 10 of You Will Share this Link without Reading It, a New, Depressing Study Says," *Washington Post*, June 16, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/06/16/six-in-10-of-you-will-share-this-link-without-reading-it-according-to-a-new-and-depressing-study/.

134 Candice Lanius, Ryan Weber & William I. MacKenzie Jr., "Use of Bot and Content Flags to Limit the Spread of Misinformation Among Social Networks: A Behavior Attitude Survey," *Social Network Analysis and Mining* (March 12, 2021), p. 2.

135 Joshua R. Minot, Michael V. Arnold, Thayer Alshaabi, Christopher M. Danforth & Peter Sheridan Dodds, "Ratioing the President: An Exploration of Public Engagement with Obama and Trump on Twitter," *PLOS ONE*, April 14, 2021, p. 2.

136 Marc-André Argentino, "Pastel QAnon," *GNET Insights*, March 17, 2021, https://gnet-research.org/2021/03/17/pastel-qanon/.

137 Ibid.

138 Brandy Zadrozny & Ben Collins, "QAnon Looms Behind Nationwide Rallies and Viral #SavetheChilren Hashtags," *NBC News*, August 21, 2020, https://www.nbcnews.com/tech/tech-news/qanon-looms-behind-nationwide-rallies-viral-hashtags-n1237722; Shayan Sardarizadeh, "What's Behind the Rise of QAnon in the UK?," *BBC News*, October 13, 2020, https://www.bbc.com/news/blogs-trending-54065470; Katrin Bennhold, "QAnon is Thriving in Germany. The Extreme Right is Delighted," *The New York Times*, October 11, 2020.

139 For example, ISIS regularly hijacked hashtags in a variety of contexts to increase exposure to its ideology and digital presence. However, the Save the Children mobilization presents a shift in the use of hashtag hijacking for propagation and an increased effectiveness as a tool for both online and offline mobilization. See Katerina Girginova, "Hijacking Heads and Hashtags," *Global-e* (2017), pp. 1-5, https://globalejournal.org/global-e/august-2017/hijacking-heads-hashtags.

140 Whitney Phillips, *The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online* (New York: Data & Society, May 2018), pp. 6-7.

141 Charles Tilly, *Regimes and Repertoires* (Chicago, University of Chicago Press, 2006), p. 35.

142 Rachel E. Greenspan, "How the Name 'Karen' Became a Stand-in for Problematic White Women and a Hugely Popular Meme," *Business Insider*, October 26, 2020, https://www.insider.com/karen-meme-origin-the-history-of-calling-women-karen-white-2020-5.

143 Alice Marwick & Becca Lewis, *Media Manipulation and Disinformation Online* (New York: Data and Society, May 15, 2017), p. 35.

144 *Doxxing* is the practice of exposing a target's personal information online. Such exposures are used to threaten targets as well as to attack and harass them in a variety of ways offline, including making threatening phone calls or sending threatening mail, attacking friends, family, or coworkers of targets, and in some cases SWATTING (calling the police / a SWAT team to a target's address through false reports of illegal activity). For more see Danielle Keats Citron, *Hate Crimes in Cyber Space* (Cambridge, MA: Harvard University Press, 2016).

145 Robert Gorwa, "Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere," Samuel Woolley and Philip N. Howard eds. Working Paper 2017.2., *Project on Computational Propaganda*, p. 17, http://comprop.oii.ox.ac.uk/.

146 Ibid., p. 5.

147 Alice Marwick & Becca Lewis, *Media Manipulation and Disinformation Online* (New York: Data and Society, May 15, 2017), pp. 38-39.

148 "A Letter on Justice and Open Debate," Harper's Magazine, July 7, 2020, https://harpers.org/a-letter-on-justice-and-open-debate/.

149 Ibid.

150 Robert Gorwa, "Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere," Samuel Woolley and Philip N. Howard eds. Working Paper 2017.2., *Project on Computational Propaganda*, p. 18, http://comprop.oii.ox.ac.uk/.

151 Emily A. Vogels, Andrew Perrin & Monica Anderson, "Most Americans Think Social Media Sites Censor Political Viewpoints," Pew Research, August 19, 2020, https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/.

152 Luiza Bandeira, Nika Aleksejeva, Tessa Knight & Jean Le Roux, *Weaponized: How Rumors about COVID 19's Origins Led to a Narrative Arms Race*, DFR Lab Report, February 2021, p. 11.

153 See, e.g., Erin Schumaker, "Mysterious Pneumonia Outbreak Sickens Dozens in China," *ABC News*, January 6, 2020, https://abcnews.go.com/Health/mystery-pneumonia-outbreak-sickens-dozens-china/story?id=68094861.

154 Garbo Gurung (@GarboHK), Twitter post, January 4, 2020; see also Luiza Bandeira, Nika Aleksejeva, Tessa Knight & Jean Le Roux. *Weaponized: How Rumors about COVID 19s Origins Led to a Narrative Arms Race*, DRF Lab Report, February 2021, p. 11.

155 Paul Farhi and Jeremy Barr, "The Media Called the 'Lab Leak' Story a 'Conspiracy Theory.' Now It's Prompted Corrections — and Serious New Reporting," *Washington Post*, June 10, 2021, https://www.washingtonpost.com/lifestyle/media/the-media-called-the-lab-leak-story-a-conspiracy-theory-now-its-prompted-corrections--and-serious-new-reporting/2021/06/10/c93972e6-c7b2-11eb-a11b-6c6191ccd599_story.html.

156 Ibid.

157 Geoff Brumfiel & Emily Kwong, "Virus Researchers Cast Doubt on Theory of Coronavirus Lab Accident," *NPR*, April 23, 2020.

158 Mia Jankowicz, "Fauci Said U.S. Government Held Off Promoting Face Masks Because It Knew Shortages Were So Bad That Even Doctors Couldn't Get Enough," *Business Insider*, June 15, 2020, https://www.businessinsider.com/fauci-mask-advice-was-because-doctors-shortages-from-the-start-2020-6.

159 Gina Kolata & Roni Cary Rabin, " 'Don't Be Afraid of Covid,' Trump Says, Undermining Public Health Messages," *New York Times*, October 8, 2020, https://www.nytimes.com/2020/10/05/health/trump-covid-public-health.html; Lawrence Wright, "The Plague Year," *New Yorker*, December 28, 2020, https://www.newyorker.com/magazine/2021/01/04/the-plague-year.

160 Robin Young & Allison Hagan, "Trump's Racial Slurs to Describe Coronavirus Put Health Care Workers, Patients at Risk," *WBUR*, June 25, 2020, https://www.wbur.org/hereandnow/2020/06/25/trump-racial-slurs-coronavirus.

161 "Covid 'Hate Crimes' Against Asian Americans on Rise," *BBC News*, May 21, 2021, https://www.bbc.com/news/world-us-canada-56218684.

162 Glen Kessler, "Timeline: How the Wuhan Lab-Leak Theory Suddenly Became Credible," *Washington Post*, May 25, 2021, https://www.washingtonpost.com/politics/2021/05/25/timeline-how-wuhan-lab-leak-theory-suddenly-became-credible/.

163 Ibid.

164 Paul Farhi & Jeremy Barr, "The Media Called the 'Lab Leak' Story a 'Conspiracy Theory.' Now It's Prompted Corrections — and Serious New Reporting," *Washington Post*, June 10, 2021, https://www.washingtonpost.com/lifestyle/media/the-media-called-the-lab-leak-story-a-conspiracy-theory-now-its-prompted-corrections--and-serious-new-reporting/2021/06/10/c93972e6-c7b2-11eb-a11b-6c6191ccd599_story.html.

165 Ibid.

166 Luiza Bandeira, Nika Aleksejeva, Tessa Knight & Jean Le Roux, *Weaponized: How Rumors about COVID 19's Origins Led to a Narrative Arms Race*, DFR Lab Report, February 2021, p. 13.

167 "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation," World Health Organization, September 23, 2020, https://www.who.int/health-topics/infodemic#tab=tab_1.

168 See discussion in Shanin Nazar & Toine Pieters, "*Plandemic* Revisited: A Product of Planned Disinformation Amplifying the COVID-19 'Infodemic,'" *Frontiers in Public Health*, July 14, 2021, https://www.frontiersin.org/articles/10.3389/fpubh.2021.649930/full.

169 Casey Newton, "How the 'Plandemic' Viral Hoax Went Viral," *The Verge*, May 12, 2020, https://www.theverge.com/2020/5/12/21254184/how-plandemic-went-viral-facebook-youtube.

170 Lukas Otto, Isabella Glogger & Mark Boukes, "The Softening of Journalistic Political Communication: A Comprehensive Framework Model of Sensationalism, Soft News, Infotainment, and Tabloidization," *Communication Theory*, 2017, p. 141, https://doi.org/10.1111/comt.12102.

171 Yimin Chen, Niall J. Conroy & Victoria L. Rubin, "Misleading Online Content: Recognizing Clickbait as 'False News,'" *WMMD '15 Conference Proceeding*, November 13, 2015, p. 15, https://dl.acm.org/doi/10.1145/2823465.2823467.

172 Ibid.

173 Ryan M. Milner, *World Made Meme: Public Conversations and Participatory Media* (Cambridge: MIT Press, 2016), p. 1.

174 Buddhika J. Jayamaha, "Social Media Warriors: Leveraging a New Battlespace," *Parameters*, December 1, 2018, p. 12, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3008&context=parameters.

175 Milner, *World Made Meme*, p. 2.

176 Ashley A. Mattheis, "Beyond the 'LULZ': Memeification as 'Meaningful' Gamification in Far-Right Content," *GNET Insights*, January 18, 2021, https://gnet-research.org/2021/01/18/beyond-the-lulz-memifying-murder-as-meaningful-gamification-in-far-right-content/.

177 Linda Schlegel, "Jumanji Extremism?: How Games and Gamification Could Facilitate Radicalization Processes," *Journal for Deradicalization*, April 26, 2020, p. 15, https://journals.sfu.ca/jd/index.php/jd/article/view/359.

178 See discussion in Mattheis, "Beyond the 'LULZ.'"

179 Matthew Hannah, "QAnon and the Information Dark Age," *First Monday*, January 15, 2021, https://firstmonday.org/ojs/index.php/fm/article/view/10868.

180 Michael Hameleers, Anna Brosius, Franziska Marquart, Andreas C. Goldberg, Erika van Elsas & Claes H. de Vreese, "Mistake or Manipulation? Conceptualizing Perceived Mis- and Disinformation Among News Consumers in 10 European Countries," *Communication Research*, April 5, 2021, p. 2, https://journals.sagepub.com/doi/10.1177/0093650221997719.

181 Hannah, "QAnon and the Information Dark Age."

182 Ibid.

183 Anti-Defamation League, "Extremists Are Using a Range of Techniques to Exploit TikTok," August 13, 2020, https://www.adl.org/blog/extremists-are-using-a-range-of-techniques-to-exploit-tiktok.

184 Isis Chong & Robert W. Proctor, "On the Evolution of a Radical Concept: Affordances According to Gibson and Their Subsequent Use and Development," *Perspectives on Psychological Science* 15:117-132 (2020), https://doi.org/10.1177/1745691619868207.

185 James J. Gibson, *The Ecological Approach to Visual Perception* (Milton Park: Taylor & Francis, 2014), p. 119.

186 Donald Norman, *The Design of Everyday Things* (New York: Basic Books, 1988), p. 9.

187 Taina Bucher & Anne Helmond, "The Affordances of Social Media Platforms," in Jean Burgess, Alice Marwick & Thomas Poell, *The SAGE Handbook of Social Media* (Thousand Oaks: SAGE Publications, 2017), pp. 233–253.

188 Ibid.

189 Ibid.

190 Ibid.

191 See, e.g., Alex Heath, "How to Get Your Old Twitter Timeline Back," *Business Insider*, March 17, 2016, https://www.businessinsider.com/how-to-turn-off-new-twitter-timeline-2016-3#twitter-has-always-displayed-tweets-in-reverse-chronological-order-so-it-can-be-kind-of-jarring-to-see-the-random-timestamps-3; J. D. Biersdorfer, "Putting Your Twitter Feed Back in Chronological Order," *New York Times*, March 21, 2016, https://www.nytimes.com/2016/03/22/technology/personaltech/putting-your-twitter-feed-back-in-chronological-order.html.

192 For discussion of the "dopamine effect," see Trevor Haynes, "Dopamine, Smartphones & You: A Battle for Your Time," *Science in the News*, Harvard University Graduate School of Arts and Sciences, May 1, 2018; Amy B. Wang, "Former Facebook VP Says Social Media is Destroying Society with 'Dopamine-Driven Feedback Loops,'" *Washington Post*, December 12, 2017; "Brain Hacking," *60 Minutes*, CBS, January 10, 2018, available at https://www.youtube.com/watch?v=awAMTQZmvPE; Daveed Gartenstein-Ross, Robin O'Luanaigh & David Jones, "*Like a Drop of Cyanide": A Strategic Framework for Addressing Hateful Conduct and Radicalization in the Canadian Armed Forces* (Washington, D.C.: Valens Global, September 2020), pp. 24-27.

193 A.K.M. Najmul Islam et al., "Misinformation Sharing and Social Media Fatigue During COVID-19: An Affordance and Cognitive Load Perspective," T*echnological Forecasting & Social Change* 159 (July 2020), https://doi.org/10.1016/j.techfore.2020.120201.

194 Francesca Comunello, Simone Mulargia & Lorenza Parisi, "The 'Proper' Way to Spread Ideas through Social Media: Exploring the Affordances and Constraints of Different Social Media Platforms as Perceived by Italian Activists," *The Sociological Review* 64:515-532 (2016), https://doi.org/10.1111/1467-954X.12378.

195 Aneesa Chishti et al., "Affordances of Credibility on Social Media," UC Berkeley School of Information, May 18, 2020, https://www.ischool.berkeley.edu/projects/2020/affordances-credibility-social-media.

196 Ibid.

197 Lee Rainie, Janna Anderson & Jonathan Albright, "The Future of Free Speech, Trolls, Anonymity and Fake News Online," Pew Research Center, March 29, 2017, https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/.

198 Christina Nemr & William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, March 2019), pp. 26-27, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

199 Diana Zulli & David James Zulli, "Extending the Internet Meme: Conceptualizing Technological Mimesis and Imitation Publics on the TikTok Platform," *New Media & Society* (December 2020), https://doi.org/10.1177/1461444820983603.

200 Imran Ahmed, *The Disinformation Dozen: Why Platforms Must Act on Twelve Leading Online Anti-Vaxxers* (London: Center for Countering Digital Hate, 2021), p. 8, https://www.counterhate.com/disinformationdozen.

201 Jean Le Roux, "South African Twitter Accounts Gamed Trending Algorithms to Promote Prank Political Hashtags," Atlantic Council's Digital Forensic Research Lab, August 19, 2020, https://medium.com/dfrlab/south-african-twitter-accounts-gamed-trending-algorithms-to-promote-prank-political-hashtags-7ad1c6cb0622.

202 Farhad Manjoo, "How Twitter Is Being Gamed to Feed Misinformation," *New York Times*, May 31, 2017, https://www.nytimes.com/2017/05/31/technology/how-twitter-is-being-gamed-to-feed-misinformation.html.

203 Christopher Schwartz & Rebekah Overdorf, "Disinformation from the Inside: Combining Machine Learning and Journalism to Investigate Sockpuppet Campaigns," *WWW '20 Proceedings*, April 2020, p. 627, https://dl.acm.org/doi/10.1145/3366424.3385777.

204 Ibid., p. 623.

205 Ibid., p. 627.

206 Ibid.

207 David Lee, "The Tactics of a Russian Troll Farm," *BBC News*, February 16, 2018, https://www.bbc.co.uk/news/technology-43093390.

208 Kristen Finklea, *Dark Web* (Washington, DC: Congressional Research Service, March 10, 2017), https://sgp.fas.org/crs/misc/R44101.pdf.

209 Ibid.

210 Matthew Hannah, "QAnon and the Information Dark Age," *First Monday*, January 15, 2021, https://firstmonday.org/ojs/index.php/fm/article/view/10868.

211 Kristen Finklea, *Dark Web* (Washington, DC: Congressional Research Service, March 10, 2017), pp. 14-15.

212 Matthew Hannah, "QAnon and the Information Dark Age," *First Monday*, January 15, 2021, https://firstmonday.org/ojs/index.php/fm/article/view/10868.

213 See discussion in Mia Bloom & Sophia Moskalenko, *Pastels and Pedophiles: Inside the Mind of QAnon* (Stanford, CA: Redwood Press, 2021); Mike Rothschild, *The Storm is Upon Us: How QAnon Became a Movement, Cult, and Conspiracy Theory of Everything* (New York: Random House, 2021).

214 See discussion in Stephanie J. Baele, Lewys Brace & Travis G. Coan, "Variations on a Theme?: Comparing 4chan, 8kun, and Other Chans' Far-Right '/pol,'" *Perspectives on Terrorism*, February 2021, p. 67, https://www.jstor.org/stable/26984798?seq=1#metadata_info_tab_contents.

215 Caitlin Dewey, "Absolutely Everything You Need to Know to Understand 4Chan, the Internet's Own Bogeyman," *Washington Post*, September 25, 2014, https://www.washingtonpost.com/news/the-intersect/wp/2014/09/25/absolutely-everything-you-need-to-know-to-understand-4chan-the-internets-own-bogeyman/.

216 Lewys Brace, "The Role of the Chans in the Far-Right Online Ecosystem," *GNET Insights*, April 1, 2021, https://gnet-research.org/2021/04/01/the-role-of-the-chans-in-the-far-right-online-ecosystem/.

217 Nick Douglas, "It's Supposed to Look Like Shit: The Internet Ugly Aesthetic," *Journal of Visual Culture* (2014), p. 335, https://doi.org/10.1177%2F1470412914544516.

218 Ethan Zuckerman & Chand Rajendra-Nicolucci, "Deplatforming Our Way to the Alt-Tech Ecosystem," Knight First Amendment Institute Blog, January 11, 2021. https://knightcolumbia.org/blog/deplatforming-our-way-to-the-alt-tech-ecosystem.

219 "What is LBRY Exactly? Is it a Protocol, an App, a Website, or a Company?," *LBRY FAQ*, n.d., https://lbry.com/faq/what-is-lbry. For more on blockchain protocols that have been employed by some platforms associated with the extreme right, see Eviane Leidig, "Odysee: The New YouTube for the Far-Right," *GNET Insights*, February 17, 2021, https://gnet-research.org/2021/02/17/odysee-the-new-youtube-for-the-far-right/.

220 Facebook, "A Further Update on the New Zealand Terrorist Attack," March 20, 2019, https://about.fb.com/news/2019/03/technical-update-on-new-zealand/.

221 Kartik Hosanagar & Alex P. Miller, "Who Do We Blame for the Filter Bubble?: On the Roles of Math, Data, and People in Algorithmic Social Systems," in ed. Kevin Werbach, *After the Digital Tornado: Networks, Algorithms, Humanity* (Cambridge: Cambridge University Press, 2020), pp. 103-21.

222 Ibid.

223 Ibid. Hosangar and Miller write: "In some contexts, algorithmic recommendations can (modestly) increase fragmentation, while in other contexts, algorithms decrease fragmentation. This is not necessarily the understanding portrayed in some popular press, which has suggested that algorithms are a (if not the) primary culprit to blame for filter bubbles."

224 Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, May 2017), pp. 1-2 & 19, https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

225 Ibid.

226 Ibid., pp. 19-26.

227 Ibid., p. 39.

228 Samantha Bradshaw, "Disinformation Optimised: Gaming Search Engine Algorithms to Amplify Junk News," *Internet Policy Review* 8:1-24 (2019), https://doi.org/10.14763/2019.4.1442.

229 Ibid.

230 *Web crawlers* are automated programs designed to navigate from website to website, cataloguing the information present on each site. The information gets added to a database that functions like an address book of relevant sites for future search results.

231 Bradshaw, "Disinformation Optimised."

232 Ibid.

233 Jonathan Hochman, "What is Search Engine Optimization Manipulation?" *National Law Review*, May 18, 2016, https://www.natlawreview.com/article/what-search-engine-optimization-manipulation.

234 Bradshaw, "Disinformation Optimised"; Hochman, "What is Search Engine Optimization Manipulation?"

235 Michael Golebiewski & danah boyd, *Data Voids: Where Missing Data Can Easily Be Exploited* (New York: Data & Society Research Institute, October 2019), p. 5, https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf.

236 Ben Buchanan et al., *Truth, Lies, and Automation: How Language Models Could Change Disinformation* (Washington, DC: Georgetown Center for Security and Emerging Technology, May 2021), p. 1, https://cset.georgetown.edu/wp-content/uploads/CSET-Truth-Lies-and-Automation.pdf.

237 Ibid.

238 Harold Furchtgott-Roth, "Facebook, Google, and Twitter: Arbiters of Truth or Threats to Liberty?," *Forbes*, November 16, 2016, https://www.forbes.com/sites/haroldfurchtgottroth/2016/11/16/facebook-google-and-twitter-arbiters-of-the-truth-or-threats-to-liberty/?sh=d3e13fa5ae38.

239 Dan Jerker B Svantesson & William van Caenegem, "Is It Time for an Offence of 'Dishonest Algorithmic Manipulation for Electoral Gain'?," *Alternative Law Journal* 42:184-189 (2017), https://doi.org/10.1177%2F1037969X17730192.

240 Ibid.

241 Harold Furchtgott-Roth, "Facebook, Google, and Twitter: Arbiters of Truth or Threats to Liberty?," *Forbes*, November 16, 2016, https://www.forbes.com/sites/haroldfurchtgottroth/2016/11/16/facebook-google-and-twitter-arbiters-of-the-truth-or-threats-to-liberty/?sh=d3e13fa5ae38.

242 While the notion of free speech protects against persecution for expressing one's opinions in a public forum, social media platforms are not public forums, but rather are private platforms that are easy for the public to access. On such platforms, a company's terms of service set the rules for what is and is not acceptable on the platform, since the platform exists on privately held property (the servers themselves and the code which operates the service), and continued usage of the platform's services implies continued agreement with these rules. The owner of the platform reserves the right to remove anyone and any content that violates the terms of service. See Brett M. Pinkus, "The Limits of Free Speech in Social Media," UNT Dallas College of Law, April 26, 2021, https://accessiblelaw.untdallas.edu/limits-free-speech-social-media.

243 Caitlin Petre, Brooke Erin Duffy & Emily Hund, "'Gaming the System': Platform Paternalism and the Politics of Algorithmic Visibility," *Social Media + Society* (October 2019), https://doi.org/10.1177/2056305119879995.

244 Ibid.

245 Brita Ytre-Arne & Hallvard Moe, "Folk Theories of Algorithms: Understanding Digital Irritation," *Media, Culture & Society* 43:807-824, https://doi.org/10.1177/0163443720972314.

246 Caitlin Petre, Brooke Erin Duffy & Emily Hund, "'Gaming the System': Platform Paternalism and the Politics of Algorithmic Visibility," *Social Media + Society* (October 2019), https://doi.org/10.1177/2056305119879995.

247 World Health Organization, "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation," September 23, 2020, https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation; Paul Barrett, "Social Media Can Be an 'Arbiter of the Truth' After All," *Politico*, April 14, 2020, https://www.politico.com/news/agenda/2020/04/14/social-media-coronavirus-184438.

248 Paul Barrett, "Social Media Can Be an 'Arbiter of the Truth' After All," *Politico*, April 14, 2020, https://www.politico.com/news/agenda/2020/04/14/social-media-coronavirus-184438.

249 Ibid.

250 Ibid.

251 We use the term *jihadist* in this report because it is an organic term: the way that those within the movement refer to themselves. However, it should be understood that the Arabic word *jihad*, which translates to *struggle*, is a well-established Islamic religious concept with many connotations. Most Muslims interpret the term in significantly different ways than do the self-proclaimed jihadists. For many Muslims, jihad is a peaceful inner struggle to live in accordance with Islam. But Islamist militant organizations that refer to themselves as *jihadist* groups emphasize the physical warfare aspect of jihad, broadly interpreting when such warfare is justified.

252 Elizabeth Bodine-Baron et al., *Examining ISIS Support and Opposition Networks on Twitter* (Santa Monica, CA: RAND, 2016), p. 1, https://doi.org/10.7249/RR1328.

253 Ibid., p. xi.

254 Mia Bloom, "No Place to Hide, No Place to Post: Lessons from Recent Efforts at 'De-Platforming' ISIS," *Just Security*, December 5, 2019, https://www.justsecurity.org/67605/no-place-to-hide-no-place-to-post-lessons-from-recent-efforts-at-de-platforming-isis/.

255 Ibid.

256 Ibid.

257 Ashley Parker, "Twitter's Secret Handshake," *New York Times*, June 10, 2011.

258 Jim Edwards. "The Inventor of the Twitter Hashtag Explains Why He Didn't Patent It," *Business Insider*, November 21, 2013.

259 P.W. Singer & Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), pp. 190-91.

260 James P. Farwell, "The Media Strategy of ISIS," *Survival*, Nov. 25, 2014, p. 51.

261 See discussion in Amanda Seitz & Ali Swenson, "Baseless Wayfair Child-trafficking Theory Spreads Online," *Washington Post*, July 16, 2020, https://www.washingtonpost.com/business/technology/baseless-wayfair-child-trafficking-theory-spreads-online/2020/07/16/f5206c10-c7aa-11ea-a825-8722004e4150_story.html.

262 Brandy Zadrozny & Ben Collins, "QAnon Looms Behind Nationwide Rallies and Viral #SavetheChildren Hashtags," *NBC News*, August 21, 2020, https://www.nbcnews.com/tech/tech-news/qanon-looms-behind-nationwide-rallies-viral-hashtags-n1237722.

263 Kevin Roose, "How 'Save the Children' is Keeping QAnon Alive," *New York Times*, September 28, 2020, https://www.nytimes.com/2020/09/28/technology/save-the-children-qanon.html.

264 Simone Rafael, "Parents Baited Through "Save the Children" Conspiracy," *Belltower News*, September 29, 2020; Marc-André Argentino, "Pastel QAnon," *GNET Insights*, March 17, 2021, https://gnet-research.org/2021/03/17/pastel-qanon/; Bloom & Moskalenko, *Pastels and Pedophiles*, pp. 57-63.

265 Rebecca Lewis, *Alternative Influence Networks* (New York: Data and Society, September 18, 2018), pp. 4-5, https://datasociety.net/library/alternative-influence/.

266 Ibid., p. 28.

267 Jack Nicas, "Alex Jones Said Bans Would Strengthen Him. He Was Wrong," *Washington Post*, September 4, 2018, https://www.nytimes.com/2018/09/04/technology/alex-jones-infowars-bans-traffic.html.

268 Lewis, *Alternative Influence Networks*, p. 40.

269 Ibid., p. 30.

270 New York State Office of the Attorney General, *Fake Comments: How U.S. Companies & Partisans Hack Democracy to Undermine Your Voice* (Albany, NY: May 6, 2021), p. 5, https://ag.ny.gov/sites/default/files/oag-fakecommentsreport.pdf.

271 Marko Kovic, Adrian Rauchfleisch, Marc Sele & Christian Caspar, "Digital Astroturfing in Politics: Definition, Typology, and Countermeasures," *Studies in Communication Sciences* (2018), p. 70, https://doi.org/10.24434/j.scoms.2018.01.005.

272 Henry Farrell and Bruce Schneier, "'Grassroots' Bot Campaigns are Coming. Governments Don't Have a Plan to Stop Them," *Washington Post*, May 20, 2021, https://www.washingtonpost.com/outlook/2021/05/20/ai-bots-grassroots-astroturf/.

273 In this context, *a pseudo-state campaign* can be thought of as an information operation that has the trappings of state involvement and is either 1) a proxy of a state, 2) sponsored and facilitated by a state, or 3) is otherwise acting on behalf of a state with the direct or tacit acknowledgement of the state. Operations that are suspected of having ties to a state but that cannot be properly confirmed or attributed can also fall into this category.

274 Sanja Kelly, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy* (Washington, DC: Freedom House, November 2017), p. 1, https://freedomhouse.org/sites/default/files/2020-02/FOTN_2017_Final_compressed.pdf; see also Carly Nyst & Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns* (Palo Alto, CA: Institute for the Future Digital Intelligence Lab, 2018), p. 8, https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf.

275 Adam Bienkov, "Astroturfing: What Is It and Why Does It Matter?," *The Guardian* (London), February 8, 2012, https://www.theguardian.com/commentisfree/2012/feb/08/what-is-astroturfing.

276 Kelly, *Freedom on the Net 2017*, p. 8; see also Nyst & Monaco, *State-Sponsored Trolling*, p. 8.

277 Nyst & Monaco, *State-Sponsored Trolling*, p. 9.

278 Ibid.

279 Ibid., p. 13.

280 For more information on the history of Soviet active measures, see Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

281 Christina Nemr & William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, 2019), p. 15, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

282 Denis Stukal et al., "Detecting Bots on Russian Political Twitter," *Big Data* 5:310-324 (December 2017), http://doi.org/10.1089/big.2017.0038.

283 Paula J. Dobriansky, "Russia's Grab for Its Neighbors," Belfer Center for Science and International Affairs, Harvard University, March 29, 2015, https://www.belfercenter.org/publication/russias-grab-its-neighbors; Nemr & Gangware, *Weapons of Mass Distraction*, p. 16.

284 Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: U.S. Department of Justice, March 2019), p. 1, https://www.justice.gov/archives/sco/file/1373816/download.

285 Ibid., p. 36.

286 APT, or Advanced Persistent Threat, refers to a threat actor, often a state actor or state-sponsored actor, that has gained persistent access to a computer system or network due to some vulnerability or a social engineering attack that tricks a user into opening a specially crafted file that runs unauthorized code on the computer system. This unauthorized code then gives the threat actor access to the computer or network. The actor retains the ability to stealthily access the system for a prolonged period and to return on subsequent visits. The number following APT refers to the order in which a threat was discovered, serving as a unique identifier of that threat actor across the information security community. CrowdStrike, "CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight," June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

287 Ibid.

288 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, p. 36.

289 "Bear on Bear," *Economist*, September 22, 2016, https://www.economist.com/united-states/2016/09/22/bear-on-bear.

290 CrowdStrike Adversary Universe, "Adversary: Cozy Bear," n.d., https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/.

291 Quoted in "Bear on Bear," *Economist*, September 22, 2016, https://www.economist.com/united-states/2016/09/22/bear-on-bear.

292 Indictment, *United States v. Internet Research Agency*, 1:18-cr-00032-DLF (D.D.C., February 16, 2018), p. 4, https://www.justice.gov/file/1035477/download.

293 Ibid., p. 12.

294 The IRA's operation is laid out in exhaustive detail in both the Department of Justice's indictment of the organization as well as the Mueller report. The activities enumerated here constitute only a small sample of the activities conducted by the IRA.

295 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, p. 14.

296 For example, one study showed that across a cohort of over 1,700 Democrats and Republicans who came in contact with IRA propaganda, no change was noted in the political behavior of these individuals. The study's authors noted that this finding suggests that "Americans may not be easily susceptible to online influence campaigns," a finding that flies in the face of much of the media coverage of Russia's 2016 IO. Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *PNAS* 117:243-250 (January 2020), https://doi.org/10.1073/pnas.1906420116.

297 Thomas Rid & Ben Buchanan, "Hacking Democracy," *SAIS Review of International Affairs* 38:3-16 (Winter-Spring 2018), https://doi.org/10.1353/sais.2018.0001.

298 Richard Tilley, "The Kremlin's Return to Active Measures," *Lawfare*, October 20, 2020, https://www.lawfareblog.com/kremlins-return-active-measures.

299 Lily Kuo, "China State Media Merger to Create Propaganda Giant," *Guardian* (London), March 21, 2018, https://www.theguardian.com/world/2018/mar/21/china-state-media-merger-to-create-propaganda-giant; Christina Nemr & William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, 2019), p. 20, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

300 Donnelle Eller, "Chinese-Backed Newspaper Insert Tries to Undermine Iowa Farm Support for Trump, Trade War," *Des Moines Register*, September 26, 2018.

301 Nemr & Gangware, *Weapons of Mass Distraction*, p. 21.

302 Luiza Bandeira et al., *Weaponized: How Rumors About COVID-19's Origins Led to a Narrative Arms Race* (Washington, DC: Atlantic Council's Digital Forensic Research Lab, February 2021), p. 33, https://www.atlanticcouncil.org/weaponized-covid19-narratives/.

303 Nemr & Gangware, *Weapons of Mass Distraction*, p. 23.

304 Ibid.

305 Kanishk Karan, Ayushman Kaul & Ben Nimmo, "Facebook Removes Iran-based Assets. Again," Atlantic Council's Digital Forensic Research Lab, May 30, 2019, https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f.

306 Quoted in Sonja Swanbeck, "How to Understand Iranian Information Operations," *Lawfare*, February 19, 2021, https://www.lawfareblog.com/how-understand-iranian-information-operations.

307 European Parliament, *Computational Propaganda Techniques* (2018), p. 1, https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf.

308 McKenzie Himelein-Wachowiak et al., "Bots and Misinformation Spread on Social Media: Implications for COVID-19," *Journal of Medical Internet Research* 23 (May 2021), https://doi.org/10.2196/26933.

309 Samuel C. Woolley, "Bots and Computational Propaganda: Automation for Communication and Control," in eds. Nathaniel Persily & Joshua A. Tucker, *Social Media and Democracy: The State of the Field, Prospects for Reform* (Cambridge: Cambridge University Press, 2020), pp. 89-110.

310 Ibid.

311 Donie O'Sullivan, "Russian Trolls Created Facebook Events Seen by More Than 300,000 Users," *CNN*, January 26, 2018, https://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html.

312 Žilvinas Švedkauskas, Chonlawit Sirikupt & Michel Salzer, "Russia's Disinformation Campaigns Are Targeting African Americans," *Washington Post*, July 24, 2020, https://www.washingtonpost.com/politics/2020/07/24/russias-disinformation-campaigns-are-targeting-african-americans/.

313 Nicholas Gueguen, "Foot-in-the-Door Technique and Computer-Mediated Communication," *Computers in Human Behavior* (January 2002), p. 11, https://doi.org/10.1016/S0747-5632(01)00033-4.

314 Ibid., p. 14.

315 Poppy Noor, "How the Alt-Right Coopted the OK Hand Sign to Fool the Media," *The Guardian* (London), October 3, 2019, https://www.theguardian.com/world/2019/oct/03/ok-sign-gesture-emoji-rightwing-alt-right.

316 Ibid. For further discussion of this hoax/trolling campaign, see Anti-Defamation League, "How the 'OK' Symbol Became a Popular Trolling Gesture," updated September 5, 2018, https://www.adl.org/blog/how-the-ok-symbol-became-a-popular-trolling-gesture.

317 UNICEF, press release, "UNICEF Poll: More Than a Third of Young People in 30 Countries Report Being a Victim of Online Bullying," September 3, 2019, https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying.

318 "Trolls and Tribulations: One-in-Four Canadians Say They're Being Harassed on Social Media," Angus Reid Institute, October 21, 2016, https://angusreid.org/social-media/.

319 Emily A. Vogels, "The State of Online Harassment," Pew Research Center, January 13, 2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

320 Megan Garber, "Doxing: An Etymology," *The Atlantic*, March 6, 2014, https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/.

321 See Nellie Bowles, "How 'Doxxing' Became a Mainstream Tool in the Culture Wars," *New York Times*, August 30, 2017, https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.

322 Tom Blackwell, "Russian Fake-News Campaign Against Canadian Troops in Latvia Includes Propaganda About Litter, Luxury Apartments," *National Post*, November 17, 2017; Marie-Danielle Smith, "Canadian Troops in Latvia Warned Their Social Media Accounts and Cell Phones Could Be 'Manipulated or Misused,'" *National Post*, November 19, 2017.

323 Tom Blackwell, "Russian Fake-News Campaign Against Canadian Troops in Latvia Includes Propaganda About Litter, Luxury Apartments," *National Post*, November 17, 2017.

324 Ibid.

325 Ibid.

326 "Igaunijā Bažījas par Krievijas Centieniem Izmantot NATO Karavīrus, lai Diskreditētu Aliansi" [Estonia is concerned about Russia's efforts to use NATO troops to discredit the alliance], *TVNet* (Latvia), February 21, 2017, https://www.tvnet.lv/4587584/igaunija-bazijas-par-krievijas-centieniem-izmantot-nato-karavirus-lai-diskreditetu-aliansi.

327 Murray Brewster, "Canadian-Led NATO Battlegroup in Latvia Targeted by Pandemic Disinformation Campaign," *CBC News*, May 24, 2020.

328 Seren Morris, "#DoctorsSpeakUp Trends on Twitter as Anti-Vaccine Movement Hijacks Hashtag Intended to Combat Misinformation," *Newsweek*, March 5, 2020.

329 Ibid.

330 Mohana Ravindranath, "Doctors Bring the Fight to Anti-Vaxxers Online," *Politico*, February 15, 2021, https://www.politico.com/news/2021/02/15/social-media-anti-vaxxers-468946.

331 Phoenix Andrews, "Social Media Futures: What is Brigading?," Tony Blair Institute for Global Change, March 10, 2021, https://institute.global/policy/social-media-futures-what-brigading.

332 Ibid.

333 Ibid.

334 Juana Summers, "Conservatives Targets of 'SWAT-ing,'" *Politico*, June 11, 2012, https://www.politico.com/story/2012/06/conservative-bloggers-targets-of-swat-ing-077292.

335 U.S. Attorney's Office, press release, "Former Atomwaffen Division Leader Sentenced for Swatting Conspiracy," May 4, 2021, https://www.justice.gov/usao-edva/pr/former-atomwaffen-division-leader-sentenced-swatting-conspiracy.

336 Ibid.

337 Ibid.

338 Yevgeny Kuklychev, "Innovative Information Disorder Tactics Target Russian Protests," *First Draft News*, February 19, 2021, https://firstdraftnews.org/articles/innovative-information-disorder-tactics-target-russian-opposition-protests/.

339 Ibid.

340 Bani Sapra, "The Last Decade Showed how Social Media Could Topple Governments and Make Social Change — and It's Only Getting Crazier from Here," *Business Insider*, January 14,, 2020, https://www.businessinsider.com/social-media-activism-facebook-twitter-youtube-power-2019-12?r=US&IR=T.

341 K. Rambo, "Protest Medics in Portland Not Spared from Force, Targeting by Police," *The Oregonian*, August 8, 2020, https://www.oregonlive.com/news/2020/08/protest-medics-in-portland-not-spared-from-force-targeting-by-police.html.

342 Jagger Blaec, "The Complicated Rise and Swift Fall of Portland's Wall of Moms Protest Group," *Portland Monthly*, August 3, 2020, https://www.pdxmonthly.com/news-and-city-life/2020/08/the-complicated-rise-and-swift-fall-of-portland-s-wall-of-moms-protest-group.

343 Chris Walker, "Portland's Wall of Moms Joined by Dads With Leaf Blowers Against Trump's Police," *Truthout*, July 21, 2020, https://truthout.org/articles/portlands-wall-of-moms-joined-by-dads-with-leaf-blowers-against-trumps-police/.

344 See discussion in Robert Evans, "Portland, Oregon, Is Ground Zero for Violent Culture-War Clashes. And It's Spreading," *Rolling Stone*, September 14, 2021, https://www.rollingstone.com/culture/culture-features/proud-boys-oath-keepers-antifa-portland-violence-spreading-1224762/.

345 Shahin Nazar & Toine Pieters, "Plandemic Revisited: A Product of Planned Disinformation Amplifying the COVID-19 'Infodemic,'" *Frontiers in Public Health* 9 (July 2021), https://doi.org/10.3389/fpubh.2021.649930.

346 Sheera Frenkel, Ben Decker & Davey Alba, "How the 'Plandemic' Movie and Its Falsehoods Spread Widely Online," *New York Times*, May 20, 2020, https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html.

347 Zarine Kharazian & Tessa Knight, "Why the Debunked COVID-19 Conspiracy Video 'Plandemic' Won't Go Away," Digital Forensic Research Lab (Atlantic Council), May 14, 2020, https://medium.com/dfrlab/why-the-debunked-covid-19-conspiracy-video-plandemic-wont-go-away-c9dd36c2037c.

348 Ibid.

349 Ibid.

350 "Anti-Lockdown Protests Have Been Hijacked by Conspiracy Theorists," *The Economist*, September 6, 2020, https://www.economist.com/international/2020/09/06/anti-lockdown-protests-have-been-hijacked-by-conspiracy-theorists.

351 Christopher Weber, "Engineer Intentionally Derails Train Near Navy Hospital Ship, Says 'USNS Mercy Was Suspicious,'" *Navy Times*, April 2, 2020, https://www.navytimes.com/news/your-military/2020/04/02/train-engineer-intentionally-derails-locomotive-near-hospital-ship-says-usns-mercy-was-suspicious/.

352 Ashitha Nagesh, "This Police-Free Protest Zone Was Dismantled – But Was It the End?," *BBC*, July 11, 2020, https://www.bbc.com/news/world-us-canada-53218448.

353 Ezra Marcus, "In the Autonomous Zones," *The New York Times*, July 1, 2020, https://www.nytimes.com/2020/07/01/style/autonomous-zone-anarchist-community.html.

354 Ibid.

355 J.M. Berger, *Extremism* (Cambridge, MA: MIT Press, 2018), p. 82.

356 It would perhaps be in poor taste to rattle off the rather striking number of anti-vax influencers who have died of COVID-19.

357 For examples of such programs, see Government of Canada, press release, "Supporting Media Literacy to Stop the Spread of Online Disinformation," October 26, 2020, https://www.canada.ca/en/canadian-heritage/news/2020/10/supporting-media-literacy-to-stop-the-spread-of-online-disinformation.html; "Help Students Fight Information Pollution," CIVIX, n.d., https://newsliteracy.ca/.

358 In the last year, there have been several examples of military personnel in Western democracies espousing extremist ideology or having connections to extremist groups. See Stewart Bell, "Extremist Groups 'Actively Recruiting' Military and Police, Canadian Intelligence Report Warns," *Global News*, August 23, 2021, https://globalnews.ca/news/8128463/extremist-groups-military-recruitment-report/; Kyle Rempfer, "Guardsman Removed from DC Mission after FBI Said Troop 'Expressed White Supremacist Ideology' Online," *Army Times*, June 5, 2020, https://www.armytimes.com/news/your-army/2020/06/05/guardsman-removed-from-dc-mission-after-fbi-said-troop-expressed-white-supremacist-ideology-online/; U.S. Department of Defense, press release, "DOD Leaders Will Address Extremism in the Ranks," February 8, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2497216/extremism-in-the-ranks-will-be-addressed-by-dod-leaders/; Daniel Boffey, "Heavily Armed AWOL Belgian Soldier Flagged as Threat in February," *The Guardian* (London), June 16, 2021, https://www.theguardian.com/world/2021/jun/16/heavily-armed-awol-belgian-soldier-jurgen-conings-flagged-threat-february. Also see discussion in a previous TEG that one of the authors of this report produced in late 2020: Daveed Gartenstein-Ross, Robin O'Luanaigh & David Jones, *"Like a Drop of Cyanide": A Strategic Framework for Addressing Hateful Conduct and Radicalization in the Canadian Armed Forces* (Washington, DC: Valens Global, September 2020).

IWC PRESS